

Blockchain, criptoactivos y metaverso

Una aproximación teórica

Narcisa Medranda Morales / Miguel Arcos Argudo

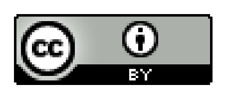




Blockchain, criptoactivos y metaverso. Una aproximación teórica

Narcisa Medranda Morales
Miguel Arcos Argudo

MEDRANDA MORALES, N., and ARCOS AGUDO, M. *Blockchain, criptoactivos y metaverso*. Una aproximación teórica [online]. Quito: Editorial Abya-Yala, 2023, 118 p. ISBN: 978-997-810-802-4. Available from: https://books.scielo.org/id/pb8tf. https://doi.org/10.17163/abyaups.6



Narcisa Medranda Morales
Miguel Arcos Argudo

Blockchain, criptoactivos y metaverso

Una aproximación teórica



2023

***BLOCKCHAIN*, CRIPTOACTIVOS Y METAVERSO**
Una aproximación teórica
© Narcisa Medranda Morales / Miguel Arcos Argudo

1ra edición: © Universidad Politécnica Salesiana
Av. Turuhuayco 3-69 y Calle Vieja
Cuenca-Ecuador
P.B.X. (+593 7) 2050000
e-mail: publicaciones@ups.edu.ec
www.ups.edu.ec

CARRERA DE COMUNICACIÓN

ISBN impreso: 978-9978-10-801-7
ISBN digital: 978-9978-10-802-4

DOI: https://doi.org/10.17163/abyaups.6

Edición, diseño, diagramación e impresión: Editorial Universitaria Abya-Yala
Quito-Ecuador

Tiraje: 300 ejemplares

Impreso en Quito-Ecuador, abril de 2023

Publicación arbitrada de la Universidad Politécnica Salesiana



Índice

Índice de figuras

Introducción

En los últimos años, la tecnología *blockchain*, las criptomonedas y el metaverso han sido temas de conversación constante entre la ciudadanía. Su impacto en diversos ámbitos ha sido significativo, y su potencial para transformar aún más la sociedad es impresionante. De hecho, se espera que el mercado de criptomonedas alcance los 5 billones de dólares para 2026, mientras que el mercado de metaversos podría alcanzar los 280 mil millones de dólares en el mismo período.

Pero, ¿qué son exactamente estas tecnologías y cómo funcionan? ¿Cómo están cambiando la forma en que interactuamos con el mundo digital y cómo pueden afectar nuestro futuro? Este libro tiene como objetivo proporcionar una aproximación teórica sobre estos temas y responder a estas preguntas.

En primer lugar, se explicará la tecnología *blockchain*, que es la base de las criptomonedas y otros sistemas de registro distribuido. Se analizará cómo funciona, cuáles son sus características y ventajas, y qué implicaciones tiene para diversos ámbitos, como la banca, la logística y la identidad digital. Además, se examinará cómo la *blockchain* está siendo utilizada para crear nuevas formas de financiamiento, como las ofertas iniciales de monedas (ICO), y cómo está impactando en el mundo de las finanzas descentralizadas (DeFi).

En segundo lugar, se abordará el tema de los criptoactivos y las criptomonedas. Se explicará qué son estas monedas digitales, cuáles son las principales diferencias entre ellas y cómo se pueden adquirir y utilizar. También se hablará sobre la volatilidad del mercado de criptomonedas y cómo ha evolucionado en los últimos años, así como su relación con las políticas monetarias y fiscales de los gobiernos.

Por último, se tratará el tema del metaverso, que es un mundo virtual en el que los usuarios pueden interactuar y realizar diversas actividades en línea. Se explicará cómo funciona esta tecnología, cuáles son las implicaciones sociales y económicas de su adopción y cómo puede ser utilizada para crear nuevas oportunidades de negocio y empleo.

En resumen, este libro proporciona una aproximación teórica y completa sobre la tecnología *blockchain*, las criptomonedas y el metaverso. A través de una combinación de datos y cifras relevantes, teoría y ejemplos prácticos, se espera que el lector obtenga una comprensión completa de estas tecnologías emergentes y su impacto en la sociedad actual y futura.

Capítulo 1

Blockchain

Origen de la *blockchain*

Si bien es cierto que el auge de la moneda digital *bitcoin* ha dado a conocer la tecnología de la cadena de bloques (*blockchain*), también lo es que las bases en las cuales se sustenta se remontan a 1991, cuando los científicos Stuart Haber y W. Scott Stornetta introdujeron la idea de una propuesta teórica con la finalidad de proporcionar una solución computacional para documentos digitales con marca en el tiempo. En este trabajo plantearon una cadena concreta de bloques protegidos mediante un criptograma.

Una *blockchain* puede ser entendida como una secuencia de paquetes de datos llamados bloques, enlazados unos a otros mediante un código criptográfico único, que contienen información en formato digital, la cual se almacena en una red colaborativa de ordenadores operada por una comunidad de personas a los que se les denomina "mineros". La principal característica de esta red radica en que todos sus nodos tienen almacenada la misma información, constituyendo una base de datos distribuida.

En 2008, Satoshi Nakamoto[1] publica el artículo *Bitcoin: A Peer-to-Peer Electronic Cash System*, en el cual se explica el funcionamiento de una versión "*peer- to-peer*" (por pares) de dinero virtual que no requiere de intermediarios ni terceras partes para realizar su registro, haciendo posible los pagos en línea (*on-line*) sin la participación de una entidad (como los bancos) u organismo central. Además, se detalla la tecnología de cadena de bloques (*blockchain*) cuya función era poner en práctica

1 Pseudónimo utilizado por la persona o las personas creadoras del *bitcoin.*

un sistema de registro de todas las transacciones de que se realizarán con estos *bitcoins,* otorgándole confiabilidad y seguridad ante la imposibilidad de falsificar las identidades y las transacciones, basados en el sistema criptográfico (Huillet, 2019). De esta manera, en enero de 2009 se realiza la primera transacción con *bitcoin.*

Para 2013, Vitalik Buterin empieza el desarrollo de una nueva plataforma de computación distribuida basada en *blockchain*, por considerar que el *bitcoin* requería un lenguaje para la creación de aplicaciones descentralizadas. Finalmente, creó su propio proyecto, dando origen a los contratos inteligentes y a *Ethereum*, la segunda moneda digital con mayor popularidad en la actualidad (Binance Academy, 2018a).

Glosario sobre *blockchain*

En esta sección se incluyen algunos conceptos básicos relacionados con la *blockchain* y las criptomonedas (basados en Vigna y Casey, 2016, citados por Arrasco, 2021), con la finalidad de facilitar la comprensión de los distintos aspectos a tratar y en los cuales se profundiza a lo largo de este trabajo.

- Base de datos centralizada: estructura de almacenamiento de datos centralizado en un solo ordenador.
- Base de datos distribuida: estructura de almacenamiento de datos almacenados en distintos ordenadores ubicados físicamente en distintos lugares geográficos.
- Bloque de recompensa (*block reward*): se refiere a la recompensa que se otorga a un minero después de haber realizado un *hash* de un bloque de transacción. Pueden ser una combinación de monedas y tarifas de transacción, dependiendo de la política utilizada por la criptomoneda en cuestión y si todas las monedas ya se han extraído con éxito.
- *Bounty*: una recompensa que se paga por completar una tarea determinada. Las tareas incluyen identificar vulnerabilidades de

código, crear contenido, trabajo de diseño, investigación, traducciones, impacto social y más.

- Cadena de bloques (*blockchain*): un libro mayor digital consensuado compuesto por datos inmutables y grabados digitalmente en paquetes llamados bloques. Cada bloque está unido al siguiente mediante una firma criptográfica, permitiendo que las cadenas de bloques actúen como un libro mayor, con la posibilidad de ser compartido y es accesible a cualquier persona con los permisos adecuados.
- Clave privada (*private key*): es una cadena alfanumérica de datos que corresponde a una sola cartera específica. Pueden considerarse como una contraseña que permite a una persona acceder a su cartera.
- Clave pública (*public key*): clave que puede ser utilizada por cualquier persona. Se utiliza para cifrar mensajes que se quieren enviar a un destinatario, quien podrá descifrarlo teniendo conocimiento de qué tipo de clave pública se trata y de su propia clave privada (*private key*).
- Contratos Inteligentes (*smart contracts*): son programas cuyos términos se registran en un lenguaje informático, en lugar de lenguaje legal. Son acciones automatizadas que se pueden codificar y ejecutar una vez que se cumple un conjunto de condiciones.
- Criptomoneda: moneda digital que se basa en las matemáticas y utiliza técnicas de encriptación para regular la creación de unidades monetarias, así como verificar la transferencia de fondos. Estas operan independientemente de un banco central.
- Dirección de cartera (*adress wallet*): se utiliza para enviar y recibir transacciones en una red *blockchain*. Una dirección es una cadena de caracteres alfanuméricos, que también se puede representar como un código QR escaneable.
- Firma digital (*digital signature*): código generado por cifrado de clave pública y adjunto a un documento transmitido electrónicamente para verificar el contenido del documento.
- Huella digital (*hash*): función que toma una entrada y, luego, genera una cadena alfanumérica conocida como "valor *hash*" o "huella

digital". Cada bloque de la cadena contiene el valor *hash* que validó la transacción antes de que siguiera su propio valor *hash*. Los *hash* confirman transacciones en la cadena de bloques

- Libro Mayor (*ledger*): es una base de datos donde se almacena toda la información de la red. Al distribuirse en muchos computadores, se garantiza que la información de dicho *ledger* sea muy difícil de modificar y *hackear*, agregando seguridad al modelo.
- Minar: proceso mediante el cual los bloques o transacciones se verifican y agregan a una cadena. Para ello, un minero debe usar una computadora (nodo) para resolver un problema criptográfico. Una vez que la computadora ha resuelto el problema, el bloque se considera "minado" o verificado.
- Moneda (*coin*): una moneda o *altcoin* es una representación del valor de los activos digitales generada a través de su propia cadena de bloques independiente.
- Nodo: cualquier computadora conectada a la red *blockchain*. Un nodo completo es una computadora que puede validar completamente las transacciones y descargar todos los datos de una cadena de bloques específica; mientras que un nodo "ligero" no descarga todas las piezas de los datos y utiliza un proceso de validación diferente.
- Oferta Inicial de Monedas (*Initial Currency Offering*, ICO): ocurre cuando una nueva criptomoneda vende *tokens* anticipados a cambio de capital inicial.
- *Token*: representa un activo construido en un *blockchain* existente. Están diseñados para ser únicos, líquidos, seguros y transferibles instantáneamente.

Tecnología contabilidad distribuida (*Distributed Ledger Technology*, DLT)

Esta tecnología es la base en la cual se sustenta la *blockchain*, aunque con sus diferencias. La tecnología contabilidad distribuida (*Distributed Ledger Technology*, DLT) es un sistema que consiste en el registro de transacciones de diferentes activos, en distintos sitios a la vez, sin

la existencia de una entidad o registro central encargado del almacenamiento, mantenimiento y administración general de todos los datos (Sáez, 2021). Este rasgo constituye la principal diferencia con los libros de registro comunes o tradicionales. En otras palabras, se trata de una gran red informática repartida en distintas ubicaciones, donde la confianza en los demás integrantes y en los datos que registran, resulta básica para el correcto funcionamiento y fiabilidad de la red.

La tecnología *blockchain* es un tipo de DLT, la cual incluye la figura de la cadena de bloques (rasgo no esencial de las DLT), con protocolos persona a persona (P2P) que garantizan la seguridad e invariabilidad de los datos contenidos en ellos (Maldonado, 2020; Sáez, 2021).

¿Qué es la *blockchain*?

Según Carlozo (2017), una *blockchain* es un libro de contabilidad digital de transacciones económicas que es totalmente público, transparente, actualizado de manera continua por innumerables usuarios, y considerado, por muchos, imposible de corromper, a través del cual se puede realizar cualquier tipo de operación entre dos personas sin que se requiera de ningún intermediario. Está conformada por una cadena cronológica de "bloques" en la que cada uno contiene un registro de la actividad de la red, donde la información pasa por un proceso de validación antes de ser registrada (Bogart y Rice, 2015), permitiendo unir datos protegidos criptográficamente. Estos bloques son únicos, inmutables, inalterables y dependientes del anterior, haciendo que no sea posible considerarlos en forma individual (Bullón Pérez *et al.,* 2020).

La *blockchain* permite la gestión de datos, órdenes, transacciones, derechos, propiedades, certificados, activos y unidades de valor certificada por los integrantes de la red (*tokens*), a través de un sistema de registro distribuido y descentralizado, los cuales se anotan en bloques de información secuenciales, que son compartidos colaborativamente entre muchos participantes de la red y verificados por los nodos que la

conforman, creándose un libro contable con copias idénticas en todos los nodos de la red (Puig, 2018).

Según Arrasco (2021), estas características son las que permiten la verificación de diferentes transacciones a lo largo del tiempo, generando seguridad y confianza en los datos almacenados, posibilitando la realización de diferentes acciones sin necesidad de la participación de un intermediario (como, por ejemplo, un banco) lo que también disminuye el coste de transacción.

La aplicación más conocida de esta tecnología está asociada a las monedas digitales o criptomonedas; sin embargo, existen diversos ámbitos de aplicación tanto en el sector público como en el sector privado, muchas de las cuales aún están por desarrollar.

Valores de la tecnología *blockchain*

Según destaca el Centro de Difusión del Conocimiento Económico (CEDICE Libertad, 2021), esta tecnología contempla valores especialmente apreciados en el sector público, a saber:

- Transparencia: en virtud de que la información almacenada en los bloques se encuentra disponible para los participantes de la cadena, o cualquier persona con acceso, en todo momento evitando la ocurrencia de operaciones indebidas dado que puede ser revisada por agentes externos, como organismos similares al Banco Mundial.
- Eficiencia: es posible trabajar con múltiples fuentes de datos y hacer más transparentes los trabajos colaborativos, mejorando el método de compartir datos y garantizando su seguridad, lo que aumenta la eficiencia de las operaciones y proyectos.
- Inclusión y control ciudadano: los ciudadanos pueden conocer directamente acerca de la información almacenada en los bloques, "mantenerse al tanto de las operaciones, proyectos o posibles irregularidades. Esta característica impulsa el control de los ciudada-

nos hacia sus gobernantes, fomenta la inclusión y disminuye los incentivos a incurrir en actos de corrupción" (p. 14).

- Descentralización: la tecnología descentraliza todas las operaciones y proyectos en los que se utiliza, ya que no depende de una autoridad central.

Elementos que conforman una *blockchain*

Teniendo presente que el propósito de la *blockchain* es proporcionar seguridad a los datos, desde este punto de vista Preukschat *et al.* (2017, p. 25) plantean que esto se logra mediante la combinación de tres aspectos: criptografía, estructura y consenso.

- Criptografía: mediante un algoritmo con clave de cifrado, un mensaje es transformado sin atender a su estructura lingüística o significado, de manera tal que sea incomprensible a toda persona que no tenga la clave de descifrado de dicho algoritmo. Además, es fundamental para evitar la manipulación, hurto o introducción errónea de información en la cadena de bloques y garantizar la generación de firmas e identidades digitales encriptadas.
- Estructura: actúan bajo las mismas reglas o protocolo para dar validez al bloque, y a la información recogida, e incorporarlo a *blockchain.* Una vez realizada esta tarea, la cadena continuará con la emisión del siguiente bloque, permaneciendo inalterable la información registrada por medio de la criptografía.
- Consenso: se sustenta en un protocolo común para la verificación y confirmación de las transacciones realizadas, asegurando su irreversibilidad. Así mismo, este consenso debe proporcionar a todos los participantes de la red una copia inalterable y actualizada de las operaciones ejecutadas.

Desde un punto de vista operativo, se puede hablar de que los elementos básicos necesarios para el funcionamiento del *blockchain* son: nodos, protocolo estándar, red de pares y sistema descentralizado.

- Nodos: pueden considerarse como los equipos informáticos de la red que sostiene la cadena de bloques, es decir, su infraestructura (Cabrera Valencia, 2018), siendo quien aporta su capacidad de procesamiento con la finalidad de ejecutar el trabajo de validación de los bloques de datos, los cuales se registran en la cadena a cambio de una retribución (criptomoneda). También, se pueden definir como los usuarios participantes en la red ejecutando el *software* y cumpliendo diferentes tareas de acuerdo con el tipo de nodo (Berryhill *et al.,* 2018 citados por CEDICE Libertad, 2021). Constituyen una red colaborativa de ordenadores, la cual se encarga del almacenamiento de datos, preservación de los registros y el resto de las acciones destinadas a garantizar la autenticidad de los mismos (Bullón Pérez *et al.,* 2020).

Existen diferentes tipos de nodos: nodos completos, nodos de minería y nodos ligeros. Los nodos completos participan en la red almacenando una copia de toda la información de la cadena, constatando y validando que no existan modificaciones en los bloques y remitiendo la información a otros nodos. Los nodos de minería, realizan estas mismas tareas y, además, generan nuevos bloques de información a la cadena con los datos validados por los nodos completos. Finalmente, los nodos ligeros solamente se encargan de enviar información a la cadena, para su validación y almacenamiento (CEDICE Libertad, 2021).

En función de la complejidad de la red, estos nodos pueden ser desde una computadora personal hasta una supercomputadora, donde se almacena el libro mayor de contabilidad (Cabrera Valencia, 2018). Independientemente de su capacidad, todas las unidades deben contar con el mismo protocolo para poder comunicarse entre sí.

- Protocolo estándar: corresponde al *software* informático, con el cual deben contar todas las computadoras que constituyen la red para poder comunicarse a través del mismo lenguaje. Su objetivo es lograr "un consenso acerca de cuál será la versión válida de registro y definir la comunicación entre los nodos" (Gómez-Cadiñanos,

2021, p. 21). Este consenso es clave para proporcionar la seguridad de los datos (Preukschat *et al.*, 2017).

- Red de pares (*Peer-to-peer*, P2P): es una red de pares compuesta por los distintos nodos, conectados e iguales entre sí, donde no existe jerarquía, pudiendo haber excepciones en el caso de las *blockchain* privadas (Puig, 2018).
- Sistema descentralizado: la red se controla de manera equivalente, ya que los participantes son iguales entre sí, por lo menos en las *blockchains* públicas (Puig, 2018).

Principios de funcionamiento de la *blockchain*

Según Catalini (2017), el funcionamiento de esta tecnología se sustenta en cinco principios básicos, a saber:

- Base de datos distribuida: debido a que cada parte de una cadena de bloques cuenta con acceso a toda la base de datos, incluyendo su historial completo, sin que exista una sola persona o entidad con el control sobre la información, lo cual implica que cada persona o entidad puede verificar de forma directa los registros de sus socios de transacciones, sin requerir de un intermediario.
- Transmisión de igual a igual: la comunicación ocurre directamente entre pares, cada nodo almacena y reenvía información a todos los demás nodos que constituyen la cadena de bloques.
- Transparencia con seudonimato: toda transacción y su valor asociado se encuentran visibles para cualquier persona con acceso al sistema. Cada nodo, o usuario, en *blockchain* cuenta con una dirección alfanumérica única de más de 30 caracteres que lo identifica. Todas las transacciones se realizan entre direcciones. Los usuarios pueden optar por mantener el anonimato o proporcionar prueba de su identidad.
- Irreversibilidad de los registros: cuando se ingresa una transacción en la base de datos y se actualizan las cuentas, estos registros no pueden ser modificados, debido a la vinculación que existe con todos los registros de transacciones anteriores (de ahí el término

“cadena”). Se implementan diversos enfoques y algoritmos computacionales para asegurarse de que la grabación en la base de datos sea permanente, ordenada cronológicamente y disponible a todos los demás en la red.
- Lógica computacional: las transacciones se pueden vincular a una lógica computacional y ser programadas, lo cual permite a los usuarios configurar algoritmos y reglas que activen automáticamente transacciones entre nodos, base de los contratos inteligentes (*smart contract*).

Funcionamiento de la *blockchain*

Sabiendo que se trata de un registro de transacciones que es compartido y verificado por los distintos participantes del sistema, el proceso a través del cual se desarrolla de manera descentralizada involucra los distintos elementos que se resumen a continuación:

- Los nodos conectados a la red descentralizada (*Peer-to-Peer)* se encargan de guardar la cadena completa que conforma la *blockchain*, almacenándose en cada uno de los integrantes de la red una copia idéntica (Romo Conde, 2021).
- Cada nodo emite diferente información (acerca de *Bitcoins*, alquileres, ventas, etc.), a la que se le denomina *token*, la cual viaja encriptada por la red, haciendo imposible que se revele el contenido.
- La red se compone de diferentes bloques, cada uno de los cuales contiene un conjunto de información verificada sobre diferentes transacciones. Estos bloques se generan a través de un *software* de código abierto y registran la información sobre cuándo y en qué secuencia se realizó la transacción, almacenando cronológicamente la información de las transacciones que se efectúan en la cadena. La programación de este *software* incluye las reglas que rigen la cadena (CEDICE Libertad, 2021).
- En cada bloque se recoge un código único de identificación con el bloque anterior, un grupo de transacciones y un código único de identificación con el bloque posterior.

- Un Brand Regular a vez que se realiza la operación en cuestión, un nodo se encarga de comprobar las transacciones y los *hash* correspondientes, encriptando esta información a través de funciones matemáticas, generando una huella digital única basada en el contenido de los bloques (Berryhill *et al.*, 2018), transformando el bloque una nueva serie de caracteres con una longitud fija (Maceo Herrera, 2021), es decir, se le otorga una identidad única e irrepetible al bloque llamada *hash*, además de un lugar específico dentro de la cadena.
- Cuando se agrega un nuevo bloque a la cadena, inicia un proceso en el que se le añade la información del *hash* del último bloque de la cadena (CEDICE Libertad, 2021). De esta manera, este *hash* queda registrado tanto en el bloque existente como en el nuevo integrante.
- El método de validación de la información se conoce como mecanismo de consenso, el cual "debe garantizar que todos los agentes del sistema puedan ponerse de acuerdo respecto a una fuente única de verdad, incluso en el caso de que algunos de ellos falle" (Binance Academy, 2018b). Según Bullón Pérez *et al.* (2020), en su mayoría, las *blockchains* utilizan dos métodos de validación de los nuevos bloques, antes de que sean incorporados a la cadena. La prueba de trabajo (*Proof of Work*, PoW) que utiliza datos difíciles de producir, pero fáciles de verificar para el resto, y la prueba de participación (*Proof of Stake*, PoS) en la cual la verificación queda a cargo de un nodo aleatorio, siempre que cumpla una serie de criterios. En todo caso, se prescinde de la necesidad de un intermediario (entidad financiera o entidad reguladora) en este proceso compartido de validación de la información a añadir.
  - En el caso concreto del *bitcoin*, el mecanismo utilizado para lograr el consenso es el PoW. Los diferentes "mineros" entran a competir entre ellos ante un problema criptográfico. El nodo que logra imponerse al resto recibe una recompensa en forma de *bitcoins*, además de las comisiones asociadas a tales transacciones (Romo Conde, 2021).

- También se tiene la prueba de autoridad (PoA), el cual es un procedimiento que genera tasas en menor tiempo que PoW. En consecuencia, las transacciones y los bloques son verificados por los "validadores", a través de fases automáticas que requieren de tres requisitos con la finalidad de asegurar su consistencia: verificación producida en la cadena; calificaciones complejas para el logro de incentivos y demostración coherente entre las investigaciones realizadas y los procesos propios (Grupo Garatu It Solutions, 2018).

• Es posible que la cadena pueda modificarse, ya sea por un cambio en las reglas de la red o debido a la solución de errores, lo que es conocido como bifurcación (*fork*), la cual establece la nueva manera como se trabajará la cadena a partir de ese momento, dividiendo la serie de bloques (Bolaños *et al.,* 2019). Los autores plantean que existen dos tipos de *fork*. Cuando las nuevas reglas o modificaciones son incompatibles con la versión precedente (*hard fork*), y cuando estas pueden coexistir con las anteriores (*soft fork*).

Tomando como resumen lo planteado por CEDICE (2021):

> En resumen, se puede decir que la tecnología *blockchain* es una red distribuida que utiliza los programas diseñados con DLT, donde cada usuario es un nodo distinto, tiene acceso a los bloques de información y, según las normas de la red, aun- que cada nodo realiza diferentes tareas, el resultado siempre es compartido. Se debe destacar que cada tarea se lleva a cabo de manera automática por el *software*, utilizando internet como recurso de conexión. (p. 10)

Tipos de *blockchain*

De acuerdo con los diferentes autores, las *blockchains* se pueden clasificar en función de las normas y propiedades que se establecen para la red. Así, se identifican dos categorías principales, a saber: según el nivel de apertura y según el nivel de permiso o accesibilidad.

Según el nivel de apertura de la red, se tienen las cadenas de bloques públicas, privadas, híbridas (federales o de consorcio) y *blockchain* como servicio (*Blockchain as Service*, BasS).

- *Blockchain* pública: permite que cualquiera pueda acceder, ver la información y hacer uso de ella dentro de la cadena, esto incluye datos, *software* y su desarrollo, donde cualquier individuo puede revisarlos, desarrollarlos y mejorarlos (CEDICE Libertad, 2021 y López Gómez-Cardiñanos, 2021). Basta descargar una aplicación y conectarse con una determinada cantidad de nodos. Se caracteriza por ser transparente, descentralizada, distribuida, consensuada y abierta (Puig, 2018) y pseudónima (los propietarios de las transacciones no son identificables de forma personal, siendo rastreables sus direcciones son rastreables por ser público). En tal sentido, estas cadenas no pueden ser anónimas, a excepción de las que expresamente se diseñan para ello (Preukschat *et al.,* 2017).
- La validación de la información se realiza a través de los nodos verificadores o mineros, quienes reciben una recompensa por cada una de las comprobaciones ejecutadas, además de las comisiones correspondientes a las transacciones. El sistema de remuneración depende de la regla de consenso (PoW, PoS, PoA) elegida para el sistema. Entre este tipo de cadenas se tienen *bitcoin*, *ethereum* y *litecoin* (todas basadas en la regla de consenso PoW) (Grupo Garatu It Solutions, 2018).
- *Blockchain* privada: solo puede ser vista por un grupo elegido de personas, debido a una serie de restricciones, tanto a la accesibilidad como al papel que desempeñan los participantes (CEDICE Libertad, 2021 y Carbonero del Val, 2021). Existe una única entidad central que ejerce control sobre las acciones que se ejecutan en la cadena: acceso a los usuarios para realizar las transacciones, acciones y base de datos, razón por la cual muchos usuarios no la consideran *blockchain* (Puig, 2019). Se caracteriza por ser cerrada, base de datos distribuida entre varios nodos (entre sus participantes o limitados a algunos de ellos) donde estos se conocen haciéndo-

se más propensa a la corrupción de datos, y anónima en cuanto a la posibilidad de establecer niveles de anonimato para realizar o proteger transacciones (Preukschat *et al.*, 2017). Este tipo de cadenas se utiliza para el intercambio de grandes volúmenes de datos, donde interesa mantener la reserva de la información. Las instituciones financieras son las que más han usado este recurso (Gutiérrez, 2019). Entre los ejemplos existentes, se pueden mencionar MONAX, Multichain, Blockstack, Ripple, Chain Quorum.

- *Blockchain* híbrida, federal o de consenso: la verificación y el encriptado de los datos es llevado a cabo por uno o varias entidades; mientras que el modelo de datos es accesible a todos con las limitaciones que estos terceros concedan a lo soliciten o, en su defecto, estará restringida solo a los participantes de la *blockchain* en ese momento. El consenso es controlado por un determinado grupo de nodos, seleccionados para tal fin (Grupo Garatu It Solutions, 2018 y Maceo Herrera, 2021). En términos generales, este tipo de cadena se utiliza por gobiernos, asociaciones y empresas (por ejemplo, del sector bancario y energético), las cuales realizan un gran número de transacciones.
- En este caso, no se asocia a criptomonedas, ni a la obtención de recompensas por el minado de los bloques (Gutiérrez, 2019). Surge con la finalidad de aprovechar los beneficios de la seguridad de la *blockchain* pública en cuanto a las dificultades para alterar los datos debido a la cantidad de nodos y la privacidad y mantenimiento controlado de la cadena privada. En definitiva, es parcialmente descentralizada y su objetivo es ofrecer un alto grado de transparencia (Maceo Herrera, 2021; Romo Conde, 2021; López Gómez-Cardiñanos, 2021).
- *Blockchain* como servicio (BasS): se refiere a una tecnología *blockchain* dispuesta en la nube, al servicio de alguna actividad. Abarca el almacenamiento de información de las transacciones, aumento de la seguridad, no requiere inversión en hardware y ofrece un entorno amigable para trabajar, siendo capaz de crear un propio canal de *blockchain* sin requerir de programación (Rodríguez, 2019).

Según el nivel de permiso o accesibilidad, se puede hablar de las cadenas de bloques abiertas (*blockchain permissionless*) en las cuales cualquier usuario puede contribuir a la generación y validación de la información, y de las cadenas de bloques cerradas o permisionadas (*blockchain permissioned*) donde solo un grupo selecto de usuarios tiene la posibilidad de realizar tales tareas (OECD, 2018).

En resumen, en la figura 1 se presenta la comparación entre los tipos de *blockchain* tomando en consideración sus diferentes características.

Figura 1

Resumen comparativo de los tipos de blockchain

	Públicos Bitcoin, Ethereum, Litecoin	Privados Hyperledger, Corda, Quorum	Federados Hyperledger, Corda, Quorum	*Blockchain as a Service* IBM, Microsoft, Amazon
Cualquiera puede participar	✓	✗	✗	NA
Los participantes actúan, en general, como nodos	✓	✗	✗	NA
Transparencia	✓	~	~	NA
Hay un único administrador	✗	✓	✗	NA
Hay más de un administrador	✗	✗	✓	NA
No hay administradores	✓	✗	✗	NA
Ningún participante tiene más derechos que los demás	✓	✗	✗	NA
Se pueden implementar Smart *Contracts*	✓	✓	✓	NA
Existe recompensa por minado de bloques	~	✗	✗	NA
Soluciona problema de falta de confianza	✓	✗	~	NA
Seguridad basada en protocolos de consenso	✓	✗	~	NA
Seguridad basada en funciones *hash*	✓	~	~	NA
Provee servicios en la nube	NA	NA	NA	✓

Nota. Tomado de Allende y Colina (2018, p. 26).

Principales usos o funcionalidades de la tecnología *blockchain*

Esta es una tecnología que se encuentra en pleno desarrollo, por lo que el gran reto en la actualidad está en afianzar las aplicaciones existentes y, más aún, en incorporar nuevos campos de acción para aprovechar los beneficios que ofrece a los distintos ámbitos de la sociedad. Por lo que, en esta sección, se exponen solo algunos de los usos más comunes.

- Criptomonedas: son "una forma de dinero efectivo digital que permite a los individuos transferir valor en un entorno digital, siendo su principal función "actuar como un sistema de dinero efectivo electrónico que no es propiedad de ninguna parte" (Binance Academy, 2018c).
- Contratos inteligentes (*smart contracts*): se trata de acuerdos entre las partes sin que exista la necesidad de un intermediario, donde la *blockchain* se utiliza con el fin de garantizar el cumplimiento de las condiciones del contrato. Su origen se ubica en los años 90, cuando Nick Szabo los concibió "como herramientas que formalizan y protegen las redes de ordenadores mediante la combinación de protocolos e interfaces de usuarios" (Binance Academy, 2019a). En el ámbito actual, se puede considerar como acuerdos digitales de obligatorio cumplimiento al cumplirse con una serie específica de reglas, predefinida a través de un código informático, el cual será replicado y ejecutado por toda la red de nodos, prescindiendo de intermediarios.
- Almacenamiento y seguimiento de datos: se pueden crear bases de datos, las cuales se modifican y observan en tiempo real (CEDICE Libertad, 2021), con aplicaciones con propósitos tan diversas, tal como lo plantean diferentes autores (Carbonero del Val, 2021; Bolaños *et al.,* 2019; Muñoz Moreno, 2020).
  - Trazabilidad: en el rastreo de productos a lo largo de toda la cadena de suministro, incluyendo detalles de ubicación, tiempos, procedencia de materiales, distribución y venta.

- Propiedad industrial e intelectual: protección del diseño y detección de falsificaciones. Mejor coordinación entre autoridades administrativas y jurídicas.
- Planificación colaborativa: ofreciendo datos confiables y en tiempo real a los participantes de la cadena, que les permita la planificación de sus actividades de manera más eficiente.
- Sostenibilidad: aportando transparencia en la información acerca de aquellos aspectos relacionados con el consumo responsable y sostenible.

Smart contracts o contratos inteligentes

Vale la pena profundizar un poco más sobre el tema de los contratos inteligentes debido a que esta es una de las aplicaciones en la que más están invirtiendo tiempo y recursos todos los entusiastas de la tecnología *blockchain.* A pesar de su nombre "contratos inteligentes" o *smart contracts*, hay quienes dicen que no se les puede llamar "contratos" debido a que por ahora todavía no tienen la característica de ser legales, y, tampoco son "inteligentes" porque su funcionamiento requiere de la aplicación de instrucciones muy básicas, a pesar de ello, los experimentos hasta ahora realizados no han tenidos los mejores resultados.

El término *smart contract* fue acuñado por Nizk Szabo en los años noventa (Kolvart *et al*., 2016) quien pensó que su uso podría optimizar los procesos relacionados con el comercio electrónico. Al estar basado en tecnología *blockchain* su funcionamiento también concibe en un registro de contratos de manera descentralizada. Todos los ordenadores de la red tendrán almacenado el código del programa de manera simultánea.

Su funcionamiento consiste en que un contrato inteligente se ejecutará de manera automática en el momento en el que se cumplan todas las condiciones estipuladas en el mismo sin que las partes puedan modificar los términos ni interrumpir su ejecución. Para ello, todos los ordenadores de la red estarán sincronizados al momento de la ejecución y todos ellos deberán obtener el mismo resultado al finalizarla.

Nótese que esta propuesta no requiere que exista un agente que ordene su ejecución ya que esto sucederá inmediatamente después de que se cumplan todas las condiciones. Ni siquiera los principales nodos de la red podrán evitar la ejecución.

Tal vez podamos comparar este tipo de contratos con una simple máquina expendedora de café. Si una persona desea tomar un café debe seguir los siguientes pasos:

- Depositar el dinero, si no lo hace la máquina no preparará el café.
- Escoger el tipo de café que desea, si no lo hace la máquina no preparará el café.
- Escoger la cantidad de azúcar, si no lo hace la máquina no preparará el café.
- Tomar su café de la máquina.

El ejemplo anterior es bastante sencillo, pero con él podemos darnos cuenta de que la máquina preparará el café únicamente en el caso de que las tres condiciones anteriores se hayan cumplido, además, una vez que la persona hay ejecutado los tres primeros pasos ya no podrá hacer nada para cancelar la preparación del café.

A continuación, se mencionan algunas características de este nuevo tipo de contratos:

- No pueden ser modificados ni siquiera en el caso de que una de las partes del contrato decida cancelar el contrato o modificar una de las cláusulas.
- Es incorruptible y una vez que se cumplan todas las condiciones su ejecución es inevitable.
- La ejecución de un contrato inteligente puede contemplar la transferencia de la propiedad de criptoactivos (como criptomonedas) de manera automática e irreversible.
- No requiere de un intermediario neutral que asuma el papel de un mediador entre las partes.

Además, los contratos inteligentes se ven beneficiados por la combinación de la tecnología *blockchain* con la inteligencia artificial. Una de las aplicaciones de la inteligencia artificial se centra en la inteligencia de negocios. Existen varios proyectos enfocados en desarrollar herramientas útiles para una gran diversidad de necesidades relacionadas a los negocios (Almonacid y Coronel, 2020). Por ejemplo, si un equipo auditor tendría la tarea de revisar manualmente los términos y condiciones de un contrato inteligente, una aplicación potenciada con inteligencia artificial podría hacerlo reportando errores, inconsistencias y vulnerabilidades en tan solo segundos.

Aplicaciones en distintos sectores

Si bien es cierto que la *blockchain* surge de la mano con el *bitcoin*, por lo que se asocia con transacciones de dinero digital, también es relevante su potencial de aplicación en una amplia gama de actividades en el sector privado, público y organizaciones no gubernamentales (ONG), tal como lo señalan autores como Maceo Herrera (2021), Carbonero del Val (2021), Muñoz Moreno (2020), Linares-Barbero (2019), Berryhill *et al.* (2018), CEDICE Libertad (2021), López Gómez-Cardiñanos (2021), entre otros, y se resumen en los siguientes aspectos:

- Transacciones financieras: permite ejecutar con mayor rapidez las transacciones con respecto a los métodos bancarios tradicionales, siendo la aplicación más consolidada de la *blockchain*.
- Automatización de la gestión de pagos y cobros, de forma simultánea: con condiciones acordadas entre múltiples participantes y previstas en contratos inteligentes, inmediatamente después de que un servicio haya sido completado.
- Comercio exterior: en automatización de los procesos entre diversos actores involucrados (compañías importadoras, exportadoras, aduanas, transportes, puertos, etc.), donde la utilización de *smart contracts* agilizaría los trámites, impulsando la competitividad.

- Ciberseguridad: en el que cada contrato almacenado dentro de la red distribuida tiene asociado un código de almacenamiento en la *blockchain*, el cual está encriptado con algoritmos seguros, lo que obstaculiza la posibilidad de cometer alguna modalidad de fraude o eliminación de los mismos.
- Telecomunicaciones: el impacto de esta tecnología en este sector económico puede ser especialmente significativo en la gestión interna de las redes, cualquier control automático o autorregulación, al reducir la complejidad de tales tareas. La evolución de la 5G, en conjunto con estructuras de redes flexibles, distribuidas y adaptables, permitirán definir diferentes tipos de redes dentro de la misma infraestructura. Esta combinación permitirá satisfacer los requerimientos técnicos demandados por los diferentes sectores, como la industria de automóviles autónomos o servicios de salud remota.
- Proveedores de servicio de Internet (ISP): podrían contar con una su red que permitirá a sus clientes demandar más recursos, cambiar la topología, ya que la *Blockchain* detectará inequívoca e inmediatamente a quien lo solicita y, en consecuencia, realizará las acciones requeridas basado en los permisos y recursos.
- Propiedad Industrial, propiedad intelectual y falsificaciones: la *blockchain* sería un avance para la protección de la propiedad industrial e intelectual, apoyando el registro de marca, manteniendo datos que permitan avalar titularidad de diseños (en fecha y hora), demostrar el momento de creación y de primera venta, facilitando la labor de documentación de las pruebas, inmediatez y ahorro en costos, utilizando los contratos inteligentes para las licencias de marca y cobro de derechos (Muñoz Moreno, 2020) y posibilitando a los consumidores para constatar la originalidad de los productos al combinarla con otras plataformas, como las de las etiquetas de identificación por radiofrecuencia utilizadas en el sector alimenticio (Linares-Barbero, 2019).

- Trazabilidad: permitiría el rastreo de los productos a lo largo de todas las actividades que conforman la cadena de suministro, pudiendo incorporarse detalles acerca de la ubicación y tiempo exacto de la producción, introducir indicadores de sostenibilidad como la procedencia de los materiales utilizados en la producción, distribución y venta (Muñoz Moreno, 2020).
- Sostenibilidad: permitiría comprobar si las materias primas provienen de un comercio justo, si los materiales ecológicos efectivamente lo son, o si se ha cumplido con los procesos de reutilización y reciclaje de materiales.
- Servicio público: la recomendación para instituciones proveedoras de servicio público son las redes *blockchain permissioned* con una combinación de acceso público y privado, ya que permiten diseñar una plataforma con diferentes tipos de agentes, desde un ciudadano que busca un servicio y registra sus datos con ese fin, hasta instituciones que requieran distintos segmentos de la información para trabajar) (Berryhill *et al.,* 2018). En este sentido, la OCDE señala que las aplicaciones más comunes en los servicios públicos son las que ofrecen una plataforma para registrar información de los usuarios:
    - Registros de identidad: como documentos de identidad, certificados de nacimiento, licencias de conducir, registros de boda, pasaportes, visas.
    - Registros personales: como registros médicos, registros criminales, registros financieros y crediticios, registros de propiedad, registros de pensión y ayuda social, registros de calificaciones y educación.
    - Registros de servicios: Como el consumo de energía, agua e internet, acceso a bienes básicos como alimentos, medicamentos y ropa.

En estos casos destaca la importancia de la segmentación de la información y el acceso que tengan los participantes en la cadena.

- Representaciones digitalizadas de documentos tradicionales de identidad: tales como licencias de conducir, pasaportes, certificados de nacimiento, registros de seguridad social, entre otros (Maceo Herrera, 2021).
- Identidad digital: constituiría la base para la integración de todos los servicios, la cual sería indispensable para ofrecer y recibir los mismos en hospitales, escuelas, bancos, empresas de electricidad, agua, telecomunicaciones, transporte, etc. (Maceo Herrera, 2021).
- Historia médica: incluiría registros médicos, farmacéuticos, consultas, tratamientos y datos de utilización de dispositivos médicos. En este último sería fundamental el registro de todos los procedimientos realizados durante una intervención quirúrgica con la asistencia de dispositivos dotados del Internet de las cosas (*Internet of things*, IoT).
- Gestión de cobros o pagos de los servicios, como pagos de peaje por autopistas, abastecimiento de combustible o pagos de factura de electricidad.
- Seguimiento de sus inventarios y donaciones en ONG y proyectos públicos: esta tecnología permitiría hacer un seguimiento de sus inventarios y donaciones, con el registro cronológico de la procedencia de un bien, su almacenamiento y, finalmente, su consumo. Además, existiría un uso único de la cadena de bloques para los fondos y proyectos públicos, haciendo transparente las transacciones, permitiendo ciudadanos y otras instituciones conozcan y verifiquen la manera como se utilizan los recursos (CEDICE Libertad, 2021).
- Internet de las cosas: estos dispositivos son fundamentales como complemento a la tecnología *blockchain*, ya que harán posible la comprobación automática de cláusulas establecidas en los contratos inteligentes, logrando acelerar, abaratar y optimizar la realización de las transacciones y el funcionamiento del *blockchain*. Los dispositivos inteligentes que envíen información a la cadena de bloques deberán contar con una identidad digital que les permita firmar digitalmente dicha información, para garantizar su confiabilidad (Maceo Herrera, 2021 y López Gómez-Cardiñanos, 2021).

Proceso de aplicación de tecnología *blockchain* en los proyectos

Los distintos aspectos asociados a la tecnología son aún desconocidos para la mayoría de las organizaciones (públicas o privadas), por lo que CEDICE Libertad (2021), ha esbozado un proceso con la finalidad de apoyar su utilización en sus proyectos, la cual se detalla a continuación:

Paso 1. Bosquejar el proyecto: se debe planificar el proyecto donde será utilizada la *blockchain,* definiendo qué se busca ofrecer o solucionar, delimitar elementos necesarios para alcanzar los objetivos, agentes involucrados y recursos disponibles para el proyecto. Por esta razón, es necesario previamente haber identificado el problema, contexto, personas afectadas y agentes intervinientes, condiciones como institución organizadora, limitaciones y capacidades técnicas para el programa y las leyes o normativas que involucran al proyecto.

Paso 2. Evaluar la aplicabilidad de *blockchain*: es necesario evaluar la efectividad de la cadena de bloques, y para ello se recomienda utilizar el diagrama presentado en la figura 2, cuyo objetivo es identificar si la tecnología *blockchain* es la herramienta más eficiente para el proyecto, ya que existen alternativas que pueden brindar mejores soluciones para ciertas tareas.

Paso 3. Ayuda profesional: contactar a quién será encargará de aplicar la cadena de bloques como herramienta para alcanzar los objetivos, ya sea contratando en la organización un equipo de programadores con experiencia en proyectos similares, o adquiriendo un servicio de terceros. La última alternativa cuenta con la ventaja de tener acceso a la experiencia de estos agentes en proyectos *blockchain*, facilitando el trabajo y aprovechando sus sugerencias para el proyecto.

Paso 4. Prueba de concepto (***Proof of concept***, PoC) ***blockchain***: en esta etapa se instrumenta, junto a los expertos, un proceso de planificación para determinar el uso de esta tecnología en el proyecto, identificando

las características únicas requeridas (normas del programa y funciones de los agentes involucrados), se establece el tipo de *Blockchain* que funciona con el proyecto (acceso público o privado, manejo de información *permissioned* o *permissionless*). Su objetivo es delimitar la aplicación de esta tecnología en el proyecto, "concretando las ideas de la institución organizadora con el apoyo del equipo de programadores y dándoles forma dentro de la cadena… (y) permite conocer de forma preliminar los posibles recursos que requiere" (p. 18).

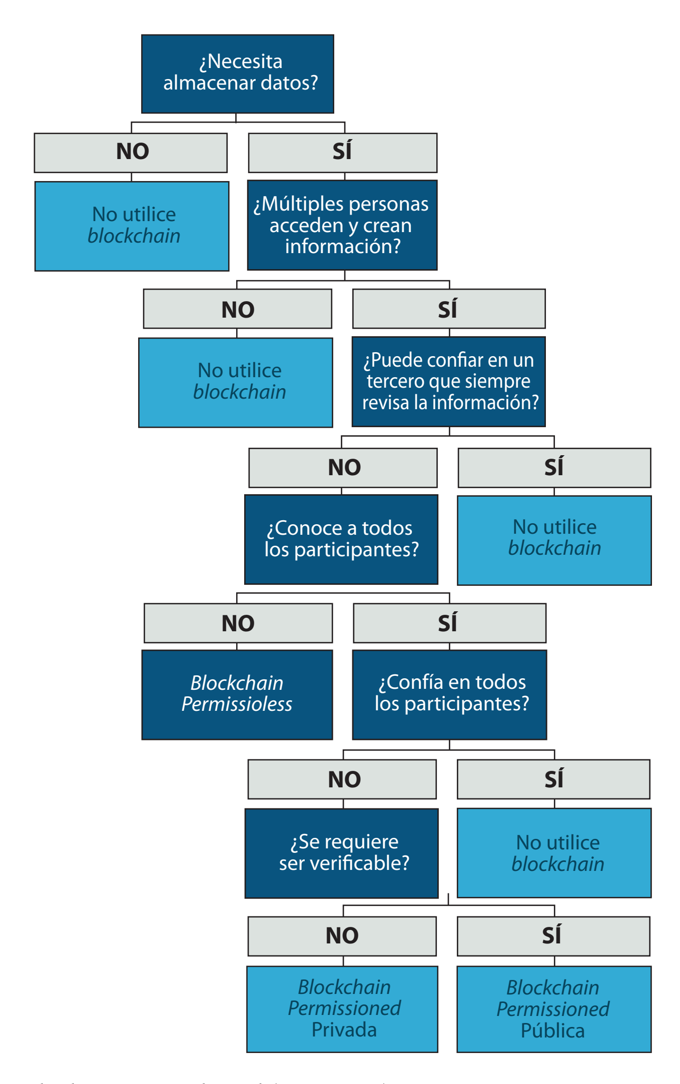
Paso 5. Producto mínimo viable: se hace una prueba del funcionamiento de la cadena, comprobando la eficiencia del programa para alcanzar los objetivos del proyecto y evaluando los costos que requiere en el tiempo para la sostenibilidad del servicio. Esto permite identificar la necesidad de realizar modificaciones antes de hacer público el programa, probándose el proyecto internamente en la institución o con la participación de un grupo selecto de usuarios y recopilando sus comentarios acerca de la experiencia. Para obtener resultados útiles, es importante definir con anticipación qué se busca evaluar con el producto mínimo viable, poniendo a prueba elementos particulares y facilitando su medición.

Paso 6. Aplicar modificaciones: se deben realizar los ajustes necesarios para lograr que el proyecto funcione eficientemente. Este paso abarca hacer cambios internos en la organización, actualizar aplicaciones asociadas a la nueva cadena, modificaciones en leyes (dependiendo de la institución organizadora) y los servicios que busque ofrecer. Una vez incorporados estos cambios, se repite el paso 5, con el objetivo de identificar la efectividad de las modificaciones y la existencia de otros aspectos a corregir.

Paso 7. Publicar el proyecto y actualizarlo: por último, se procede a permitir el acceso del público al proyecto y permanecer en constante contacto con las personas a fin de evaluar su satisfacción para evaluar si es necesario introducir modificaciones, volviendo a los pasos 5 y 6 antes de proceder a actualizar el programa al que tienen acceso.

Figura 2

Diagrama para evaluación de aplicabilidad de la tecnología blockchain en un proyecto



Nota. Tomado de CEDICE Libertad (2021, p. 17).

Ventajas y desventajas de la *blockchain*

Como es habitual, toda tecnología conlleva ventajas y desventajas que deben tenerse en cuenta al momento de su aplicación. En tal sentido, los siguientes son los aspectos más importantes relacionados con la cadena de bloques (Binance Academy, 2018d).

Ventajas

- Naturaleza distribuida: como los datos de una *blockchain* se almacenan en miles de dispositivos en una red distribuida de nodos, el sistema y los datos son altamente resistentes a fallos técnicos y ataques maliciosos. Cada nodo es capaz de replicar y almacenar una copia exacta de la base de datos y, en consecuencia, la desconexión de uno o más nodos no afecta la disponibilidad de la información ni la seguridad de la red.
- Estabilidad: una vez los datos se han registrado en la *blockchain*, es en extremo difícil eliminarlos o cambiarlos, haciendo que esta tecnología sea ideal para el almacenamiento de registros financieros o cualquier otro tipo de datos que requieren pistas de auditoría (trazabilidad), ya que todos los cambios son rastreados y permanentemente registrados en un libro contable (*ledger*) distribuido y público.
- Sistema *Trustless* (no requiere confiar en terceros): cuando se utiliza tecnología *blockchain*, no es necesaria la intervención de un intermediario para la realización de las transacciones debido a que la red de nodos distribuida se encarga de verificarlas mediante un proceso denominado minado, evitando el riesgo de tener que confiar en una organización individual y reduciendo los costos generales y comisiones por transacción.
- Compatibilidad con otras herramientas y plataformas: es compatible con otras herramientas y plataformas, permitiendo que el programa de la cadena acceda a información almacenada en otras plataformas, como bases de datos tradicionales u otras *blockchains*, o en caso

inverso, brinde información a externos, generando un ambiente de trabajo híbrido (Berryhill *et al.,* 2018; Lindman *et al.,* 2020).

Desventajas

- Ataques del 51 %: existen algunos tipos de ataques potenciales que se pueden presentar contra las *blockchains*, siendo uno de los más debatidos el relacionado con el algoritmo de consenso PoW que protege la cadena de bloques de *bitcoin*. Este tipo de ataque puede darse "si una entidad logra hacerse con el control de más del 50 % del *hashing power* (o tasa de *hash*) de la red" (Binance Academy, 2018d), permitiéndole eventualmente desorganizar la red a través de la exclusión o modificación intencionada del orden de las transacciones. Aunque este es un riesgo posible desde un punto de vista teórico, nunca se ha producido con éxito. A medida que la red crece, la seguridad se incrementa, resultando bastante improbable que los mineros empleen grandes cantidades de dinero y recursos en atacar *bitcoin*. En todo caso, una intervención de esta naturaleza solo podría modificar las transacciones más recientes durante un corto tiempo, debido a que los bloques se vinculan mediante pruebas criptográficas, donde la modificación de los bloques más antiguos requeriría niveles inasequibles de potencia computacional.
- Modificación de datos: una vez que se añaden los datos a los bloques, es muy difícil modificarlos. Aunque la estabilidad es una de las ventajas de las *blockchains*, en ocasiones puede requerirse cambiar o corregir alguno. El cambio de datos o código es habitualmente muy complicado y, a menudo, requiere de una *hard fork* abandonando una cadena y una nueva es retomada.
- Claves privadas: la *blockchain* utiliza criptografía de clave pública (también denominada asimétrica) para otorgar a los usuarios la propiedad de las unidades de su criptomoneda (o cualquier otro dato de la cadena de bloques). Cada cuenta de la *blockchain* (o dirección) dispone de dos claves: una clave pública (que se puede compartir) y una clave privada (que debe mantenerse en secreto). Los usuarios

necesitan sus claves privadas para acceder a sus fondos, actuando como su propio banco. Si un usuario pierde su clave privada, perderá también su dinero, sin poder hacerse nada al respecto.

- Ineficiencia: las *blockchains*, en especial las que usan PoW, son altamente ineficientes. Dada la competitividad del minado y que solo hay un ganador cada diez minutos, el trabajo de los demás mineros se desperdicia. El aumento de la potencia computacional de los mineros para tener mayores probabilidades de encontrar el *hash* de un bloque válido ha incrementado considerablemente los recursos utilizados por la red *bitcoin*, al punto de que en la actualidad consume más energía que muchos países como Dinamarca, Irlanda o Nigeria.
- Almacenamiento: los libros contables (*ledgers*) de la cadena de bloques pueden crecer mucho con el paso del tiempo. La de *bitcoin* requiere actualmente alrededor de 200 GB de almacenamiento. El actual crecimiento del tamaño de la *blockchain* parece estar superando al de los discos duros, por lo que existe el riesgo de que la red pierda nodos si el *ledger* se vuelve demasiado grande para ser descargado y almacenado por individuos.
- Infraestructura de telecomunicaciones: la implementación a gran escala de la tecnología necesitará de una infraestructura de telecomunicaciones capaz de suplir los requerimientos del servicio entre todos los participantes de la red (Maceo Herrera, 2021).

En resumen, la tecnología de *blockchain* se encuentra en pleno desarrollo, con un amplio potencial de aplicación en una variedad de sectores, industrias y actividades, cuyas virtudes pueden realizar aportes importantes en materia de transparencia y seguridad, especialmente en el manejo de recursos ámbito de lo público y organizaciones no gubernamentales.

Sin embargo, no está exenta de debilidades y riesgos. Temas como el anonimato (o seudoanonimato), la ineficiencia en la utilización de los recursos particularmente los energéticos, la inversión en adquisición en infraestructura tecnológica y la accesibilidad real de personas e instituciones para incorporarse a esta nueva dinámica, están apenas por empezar.

Capítulo 2
Criptoactivos y criptomonedas

Definición de criptoactivos y criptomonedas

Al investigar en la definición del término criptomoneda, es posible encontrar cómo ha ido permeando en instituciones de diversos ámbitos. Así, el diccionario de la Real Academia de la Lengua Española (RAE) incluye la definición de criptomoneda, admitiendo su origen en la combinación de cripto y moneda, derivado del término en inglés *cryptocurrency*, siendo "moneda virtual gestionada por una red de computadoras descentralizadas que cuenta con un sistema de encriptación para asegurar las transacciones entre usuarios" (Real Academia de la Lengua Española, 2022).

Un criptoactivo es un tipo de activo cuya información se encuentra almacenada en una base de datos distribuida o *blockchain*. Por ejemplo, el título de propiedad de una casa se encuentra registrado en la entidad que controla la información de la propiedad privada de una ciudad; en el caso de los criptoactivos esta información se registra por replicado en el conjunto de computadores de la red.

Según el Banco Central Europeo, "es la representación digital de valor, no emitida por ninguna autoridad central, institución de crédito o emisor de dinero electrónico reconocido que en ciertas ocasiones, puede ser utilizada como medio de pago alternativo al dinero" (European Central Bank, 2015, p. 25).

Según Fernández *et al.* (2021), en Colombia el Banco de la República reconoce los términos de criptoactivo y criptomoneda, aun cuando no los acepta como monedas, otorgándole valor solo como medio de

transferencia de activos, remitido a un mercado digital con costos menores y mayor rapidez. Esta entidad adopta de Arango *et al.* (2018) la posición de acuerdo con la cual define los criptoactivos como una referencia "particular de lo que se conoce como monedas virtuales. Estas se definen como unidades digitales susceptibles de ser usadas como medio de pago en el intercambio de bienes y servicios, como depósito de valor y como unidad de cuenta" (p. 4); donde los participantes intervienen con propósitos diversos y son responsables por las ganancias y pérdidas de este mercado, sin las garantías derivadas del respaldo de las políticas públicas.

En general, el término criptoactivos se utiliza como sinónimo de criptomonedas, y constituyen unidades digitales emitidas por agentes privados. Se expresan en su propia unidad de cuenta, las cuales son susceptibles de ser adquiridas, preservadas y transferidas de forma electrónica. A pesar de que estos términos suelen utilizarse de manera indistinta, algunos autores plantean sus reservas al respecto, debido a que mantienen la imposibilidad de considerarlas como monedas en virtud de que "al menos en su estado actual, tienen serias deficiencias para cumplir las funciones del dinero (medio de cambio, depósito de valor o unidad de cuenta)" (Parra *et al.*, 2019, p. 4).

Adicionalmente, existen otras formas o medios de cambio de naturaleza digital que no se corresponden con las denominadas criptomonedas, como aquellas creadas en ambientes específicos y, en consecuencia, de acceso limitado, usualmente controlado de manera centralizada, entre las que se encuentran las de las plataformas de entretenimiento digital o de interacción social o comercial (Halaburda y Sarvary, 2016).

Según Binance Academy (2018d), el nombre de criptomoneda corresponde a un acrónimo que se deriva de las palabras criptografía y moneda, sobre la base del uso extensivo de técnicas criptográficas utilizado para la protección de las transacciones entre usuarios.

Una criptomoneda (o "cripto" como también se le conoce) "es una forma de dinero efectivo digital que permite a los individuos transferir

valor en un entorno digital", cuya principal característica está asociada a su carácter descentralizado, donde no existe un banco central o subconjunto de usuarios con capacidad para cambiar las reglas sin alcanzar consenso previo Binance Academy (2018b). Las características de estas criptomonedas implican, en principio, la posibilidad de realizar transacciones, locales o transfronterizas, con seguridad y anonimato (o seudonimato).

Desde su creación, la intención se ha centrado en que su control se realice de forma distribuida como alternativa a las monedas fiduciarias de curso legal o *(fiat)* utilizadas habitualmente en todo el planeta y al sistema financiero actual, por lo que la popularización de la tecnología del DLT y su expresión en las *blockchains*, vino en 2009 de la mano con la aparición del *bitcoin*, la primera criptomoneda (Parra *et al.*, 2019; Rodríguez, 2019).

En este mercado, a los criptoactivos diferentes al *bitcoin* se les conoce como *altcoin,* término que se refiere a las monedas alternativas (*alternative coin*). Estas surgen con la aparición de *ethereum* en 2013 y han ganado importancia, tanto en volumen de negociación y capitalización bursátil (Binance Academy, 2021; Fernández *et al.*, 2021).

Otra manifestación de las monedas digitales se encuentra en forma de Ofertas Iniciales de Monedas (ICO, por sus siglas en inglés), las cuales tratan de asimilarse a la típica emisión de acciones en una salida a bolsa, aunque autores como Rodríguez (2019) consideran un error tal denominación debido a que en estas operaciones no se realizan emisiones de monedas o criptomonedas, sino los denominados *tokens* que, "a diferencia de las criptomonedas puras como el *bitcoin,* suelen conceder diversos derechos por lo que se les denomina criptoactivos" (p. 1).

Al principio, estos *tokens* otorgaban derechos que permitían el uso de servicios en una determinada red o una plataforma tecnológica, pero rápidamente se realizaron emisiones que dieron "lugar a instrumentos que concedían derechos que les hacían guardar gran similitud con valores negociables tradicionales como pueden ser las acciones o las obligaciones" (Rodríguez, 2019, p. 1).

Características de los criptoactivos

Las características de los criptoactivos se corresponden con las anteriormente descritas en relación al funcionamiento de las cadenas de bloque (*blockchains*), donde la validación y el registro de las transacciones se realiza de forma distribuida (cada criptoactivo usa un sistema de registro, su propio *blockchain*) entre sus participantes, y asegurado a través de técnicas de encriptado, cifrado o codificación. Al respecto, Parra *et al.* (2019) destacan que la intención más importante para los promotores de los criptoactivos es que permitan crear y mantener un sistema de transferencia de valor que, al igual que el sistema tradicional, se base en la confianza, pero en el que, a diferencia de aquel, esta no descansa en autoridades centrales (gobierno o banco central), sino que se genere a partir de las características antes mencionadas. Además, estas aportan ventajas asociadas a los costos, verificación de datos, escalabilidad, así como de los riesgos de fraude, entre otros (Fernández *et al.*, 2021).

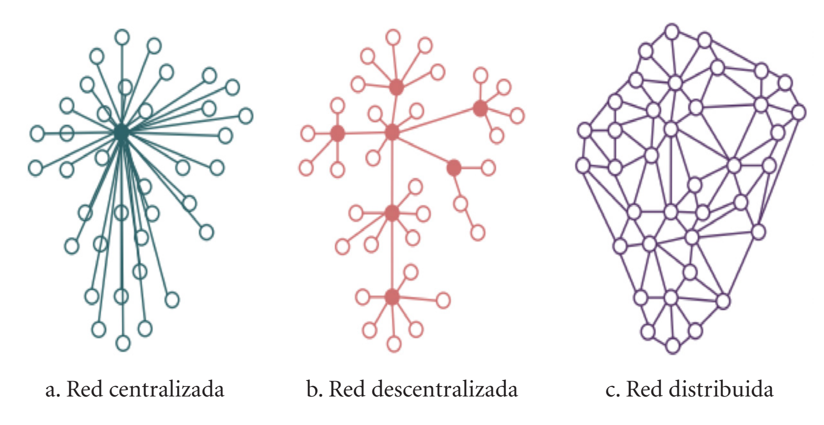
Según Lamothe y Lamothe (2020), en general, todas las criptomonedas responden a los siguientes puntos: redes descentralizadas (no controladas por ninguna autoridad), transacciones totalmente anónimas y realizables en cualquier momento, transparencia otorgada por la tecnología *blockchain* la cual registra y mantiene abierta la historia de las transacciones, costos de transacción reducidos en virtud de la ausencia de intermediarios, y transacciones rápidas e irreversibles.

Estructura del sistema de criptoactivos

El tema de la estructura de las redes utilizada para la realización de las transacciones es fundamental en la dinámica de las criptomonedas. El sistema financiero tradicional se considera como una estructura descentralizada, el cual cuenta con un reducido número de agentes conformado por los bancos centrales y demás instituciones financieras, las cuales “concentran la emisión e intercambio de activos, el procesamiento y registro de transacciones, así como la información de los usuarios” (Parra

et al., 2019, p. 8). Mientras que el diseñado por Nakamoto (2008) fue concebido como una red distribuida una red de intercambio persona a persona (*peer to peer*) entre los usuarios que la conforman, quienes, a su vez, mantendrían el registro de sus transacciones (figura 3).

Figura 3
Tipos de redes por centralización



Nota. Tomado de Parra *et al.* (2019, p. 8).

Esta misma configuración le otorga la característica de independiente, en virtud de no requerir la intervención de bancos centrales, gobiernos o instituciones financieras, sin el riesgo de que la ocurrencia de puntos únicos de falla (*single point of failure risk*) produzca pérdidas de los registros, ya que los usuarios son quienes mantienen el acceso a sus activos, cuentan con las bases de datos y realizan las transacciones directamente entre ellos (Parra *et al.*, 2019; Binance Academy, 2018c).

A pesar de su concepción original y que la mayoría de los criptoactivos basan sus operaciones en el registro distribuido, la situación no es la misma para los usuarios. Realmente estos realizan sus operaciones a través de una estructura descentralizada, concentrada en un número reducido de agentes, entre los que se destacan las plataformas de inter-

cambio y las billeteras digitales (Moore y Christin, 2013; Böhme, *et al.*, 2015; Floyd, 2018, citados por Parra *et al.*, 2019), los cuales en definitiva ejecutan actividades custodia e intermediación, similar a las entidades bancarias, con la diferencia de que se remiten solo a entornos digitales.

Además, dado que es posible comprar criptoactivos mediante transacciones compraventa con moneda fiduciaria, no es tan cierto hablar de un sistema de criptoactivos independiente del sistema financiero tradicional, debido a la interoperabilidad que, con este último sistema, requieren actualmente las plataformas de intercambio para materializar las transacciones.

Sin embargo, autores como Parra *et al.* (2019) señalan que "esta estructura descentralizada y dependiente no solo contradice el concepto (la intención) que respalda la existencia misma del sistema de criptoactivos, sino que trae consigo riesgos y retos que deben ser identificados y manejados" (p. 9).

Ofertas iniciales de criptomonedas

Según Lamothe y Lamothe (2020), la Oferta Inicial de Criptomonedas, ICO (*Initial Currency Offering*, por sus siglas en inglés), corresponde a la emisión de *utility tokens,* los cuales "son unidades de valor que pueden dar a su usuario el derecho a utilizar un producto o servicio específico y que se utilizan también para dinamizar un ecosistema" (p. 71); mientras que autores como Rodríguez (2019) extienden el término a emisiones iniciales de las denominadas criptomonedas puras como el *bitcoin* y las *altcoins,* y otros tipos de *tokens*, a saber:

- *Payment/Exchange Tokens* o criptomonedas puras: como el *bitcoin* y las *altcoins*, cuya función fundamental es servir de medio para la realización de intercambios.
- *Utility Tokens*: corresponde a aquellos instrumentos que otorgan acceso a una red o a una plataforma tecnológica o a un servicio que estas proporcionen, tal como lo señalan Lamothe y Lamothe (2020).

- *Security Tokens*: corresponde a instrumentos que se pueden asimilar a valores negociables por contar con características equivalentes a ellos (como, por ejemplo, proporcionar una participación en las utilidades de un negocio, otorgar derechos sobre la gestión de una compañía o un interés prefijado). En tal sentido, estos se consideran una inversión.
- Híbridos: son principalmente aquellos *tokens* con características de *utility* y de *security*. En general, es posible afirmar que la naturaleza de *utility* se suele ver contaminada cuando el objetivo de la emisión es financiar un proyecto empresarial, por lo que es probable que las autoridades estimen la prevalencia como valor negociable.

Monedas digitales y monedas virtuales

Aunque usualmente se asocia con las criptomonedas, su concepto es mucho más amplio. De acuerdo con la Financial Action Task Force (2014), el término "moneda digital puede hacer referencia a una representación digital de cualquier moneda virtual (no dinero fiduciario) o de dinero electrónico (dinero fiduciario)" (p. 4), razón por la cual con frecuencia suele utilizarse de manera indistinta con el término "moneda virtual".

Al establecer el concepto moneda virtual, esta se refiere a:

> Una representación digital de valor que puede ser comerciada digitalmente y funciona como (1) un medio de cambio; y/o (2) una unidad de cuenta; y/o (3) un depósito de valor, pero no tiene curso legal (es decir, cuando se ofrece a un acreedor, es una oferta válida y legal de pago) en ninguna jurisdicción. Ninguna jurisdicción emite o garantiza las monedas virtuales, y cumple con las funciones antes mencionadas por común acuerdo de la comunidad de sus usuarios. (Financial Action Task Force, 2014, p. 4)

La diferencia fundamental entre la moneda virtual y el dinero fiduciario (moneda real, dinero real, o moneda nacional), en que este último funciona de igual manera que la moneda y el papel moneda de un país designado como dinero de curso legal, el cual circula, se utiliza y

acepta como medio de intercambio en el país que lo emite. También se considera diferente del dinero electrónico, el cual:

> Es una representación digital del dinero fiduciario usado electrónicamente para transferir el valor denominado en dinero fiduciario. El dinero electrónico funciona como un mecanismo de transferencia digital para el dinero fiduciario, es decir, transfiere electrónicamente un valor que tiene la condición de moneda de curso legal. (Financial Action Task Force, p. 4)

Esta institución establece claramente los distintos tipos de monedas virtuales, distinguiendo las monedas virtuales centralizadas y las descentralizadas:

- Monedas virtuales centralizadas: cuentan con una autoridad administrativa única (administrador) o tercera parte encargada de controla el sistema. Este administrador emite la moneda, establece las normas que rigen su uso, mantiene un libro de contabilidad central de pago, y tiene autoridad para canjear (retirar) la moneda de la circulación.
- Monedas virtuales descentralizadas: conocidas como criptomonedas, "son monedas virtuales de código abierto fundamentadas matemáticamente que funcionan en una red de pares distribuida, sin autoridad central administradora, de vigilancia o de supervisión" (p. 5).

Monedas de bancos centrales

Cuando se habla de una moneda digital de banco central (Central Bank Digital Currency, CBDC), se refiere a una forma digital de dinero fiduciario (*fíat*), es decir, una moneda virtual centralizada establecida como dinero por la regulación del gobierno, declaradas de curso legal, las cuales pudieran basarse en la tecnología *blockchain* o en registros de bases de datos centralizadas por el ente emisor. Bancos centrales en diversos países están avanzando en este sentido: China trabaja desde 2014 en un proyecto denominado DC/EP —siglas que se corresponden con

“Digital Currency/Electronic Payments” y un programa activo de prueba del yuan digital, el Banco Central Europeo (BCE) propuso un euro digital en octubre de 2020 (Binance Academy, 2021b) y en Venezuela entró en circulación el bolívar digital en octubre de 2021 junto con una expresión monetaria impresa (Presidencia de la República, 2021).

Para Bech y Garratt (2017), estas CBDC se caracterizan por contar con un emisor (banco central u otro tipo); formato (electrónico o físico); accesibilidad (universal o restringida); y mecanismo de transferencia (centralizado o descentralizado).

Según Binance Academy (2021b), “desde el punto de vista tecnológico, una CBDC es básicamente una base de datos ejecutada y controlada por el gobierno (o, posiblemente, entidades autorizadas del sector privado)”, constituyéndose en una base de datos “permisionada”, en la cual solo los agentes autorizados cuentan con la capacidad de realizar las transacciones en la red, donde la entidad autorizada para controlar la base de datos también puede evitar el procesamiento de transacciones, revertirlas, “congelar” fondos o establecer direcciones en listas negras.

También plantea que muchas CBDC operarán, probablemente, en sus propias *blockchains* o podrían ser emitidas en *blockchains* públicas, lo cual permitiría disponer de activos permisionados liquidados en una capa base (*base layer*) no permisionada, donde la capa permisionada podría proporcionar a los bancos centrales el control necesario, mientras que la capa no permisionada aportaría las garantías de seguridad más elevadas. No obstante, cada país desarrollará sus sistemas según las condiciones que establezcan a tal efecto.

Entre los beneficios de estas monedas digitales de bancos centrales se encuentran la posibilidad de lograr la bancarización de la población fuera del sistema financiero, la revisión del sistema monetario en busca de una mayor eficiencia e inmediatez y la identificación de actividades ilícitas como el lavado de dinero y el financiamiento al terrorismo (Allende y Colina, 2018; CEDICE Libertad, 2021; Financial Action Task Force, 2014; Binance Academy, 2021b).

Criptomonedas vs. monedas

El uso de las criptomonedas en contraposición a las monedas tradicionales está lleno de controversia, basada en las características básicas (medio de cambio, unidad de cuenta y depósito de valor) que se esperan de estas. Así Rodríguez (2019), las puntualiza de la siguiente manera:

- Medio de cambio: una moneda debe servir como medio de pago al momento de adquirir bienes o servicios, realizar inversiones o cancelar o reducir deudas u otros tipos de obligaciones. En el caso de las criptomonedas no cumplen con esta característica, al menos no de forma plena, debido a que su aceptación para la adquisición de productos es limitada, básicamente dependiente de la voluntad del vendedor y, al no tratarse de una moneda de curso legal, no es obligatorio aceptarlas como pago frente a obligaciones de pago o deudas.
- Unidad de cuenta: la extrema volatilidad mostrada por el valor de las criptomonedas en los últimos años, representa un obstáculo para considerarlos como una unidad de cuenta estable, por lo que instituciones como el Fondo Monetario Internacional (FMI) han alertado a algunos países acerca del riesgo que estas representan (El Economista, 2022).
- Depósito de valor: esta característica de las monedas se dificulta, debido a la volatilidad antes mencionada.

Tal como señala Rodríguez (2019), en el ámbito internacional no se ha logrado alcanzar consenso acerca de la naturaleza de las criptomonedas. Algunos países las consideran activos financieros de solo desde el punto de vista bancario (Alemania), otros como una *commodity* (en Estados Unidos, aunque la acepción de este término es muy amplia e incluye activos financieros, monedas o materias primas), El Salvador ha adoptado el *bitcoin* como moneda de circulación legal y los bancos centrales o las instituciones supervisoras bancarias ponen el acento en señalar que no son divisas. En tal sentido, este tema aún está lejos de definirse.

Tipos de criptomonedas

En la actualidad existe una gran cantidad de criptomonedas, desde el *bitcoin* hasta la diversidad de *altcoins* que se han creado y siguen creándose (Binance Academy, 2021a). A continuación, se incluyen las *altcoins* más representativas, dejando una sección posterior para profundizar en lo concerniente al *bitcoin.*

Ethereum (ETH)

Es una criptomoneda creada en 2013 por el programador ruso Vitalik Buterin y lanzada oficialmente al mercado en 2015. *Ethereum* se define a sí misma en su página web como:

> Una tecnología que te permite enviar criptomonedas a cualquier persona por una pequeña comisión. También potencia aplicaciones que cualquiera puede usar y nadie puede derribar… es un mercado de servicios financieros, juegos y aplicaciones que no pueden robar tu información o censurarte. (Ethereum, 2022)

A diferencia del *bitcoin*, puede ser programable, lo que permite utilizarla para diferentes tipos de activos digitales (figura 4).

Figura 4
Logotipo de ethereum



Nota: Tomado de https://logos-marcas.com/ethereum-logo/

Según Preukschat (2017), Ethereum está basado en lenguajes de programación Turing completo, lo cual implica que todo aquello que se puede desarrollar con un leguaje se podrá también hacerlo con otros, la única diferencia podría ser el código fuente y el rendimiento de la aplicación distribuida. Se diferencia de otras criptomonedas en el hecho de que toda su información no se sitúa físicamente en ningún servidor, disminuyendo los riesgos de censuras o problemas técnicos (*Ethereum*, 2022; López Gómez-Cadiñanos, 2021).

Distintos autores como Romo Conde (2021), López Gómez-Cadiñanos (2021), Fernández *et al.* (2021), Bit2me Academy (s.f.), entre otros, han puntualizado algunas de sus características, entre las que se pueden mencionar:

- Propio lenguaje de programación "*Solidity*": que le permite una implementación mucho más sencilla, que facilita llevar a cabo los contratos inteligentes (*smarts contracts*) así como aplicaciones descentralizas que utilizan *blockchain*, permitiendo el contacto y la negociación segura entre los usuarios sin necesidad de contar con la presencia de un organismo o entidad central que los gestione (Bit2me Academy, s.f.; Romo Conde, 2021).
- Criptoactivo propio: *Ether* (ETH). Se trata de la segunda moneda digital en volumen de capitalización, la cual puede además utilizarse para ejecutar transacciones de *tokens* no fungibles (*Non-Fungible Token*, NFT).
- Mecanismo de generación de bloques: utiliza la prueba de trabajo (PoW).
- No existe una cantidad máxima de generación de *ether*, a diferencia del *bitcoin*. En términos relativos, el crecimiento de la oferta es suavemente decreciente y al llegar a 72 millones de unidades, esta se mantendrá en un máximo anual de 18 millones de nuevas monedas (Fernández *et al.*, 2021).

- Velocidad de las transacciones: en *Ethereum* las transacciones se realizan en 12 segundos y su costo se basa en los recursos que se han utilizado en la red (López Gómez-Cadiñanos, 2021).

Según Fernández *et al.* (2021), esta plataforma cuenta con diversas ventajas, siendo dos las más relevantes: primero, los contratos inteligentes a través de los cuales se establecen condiciones cuyo cumplimiento llevan a la ejecución automática de las transacciones, pudiéndose crear pago de suscripciones; segundo, que no solo se trata de una criptomoneda, se trata de una comunidad abierta (no solo de código abierto) que la utiliza para crear aplicaciones entre otros usos. Entre sus desventajas se encuentra el uso de la PoW por la ineficiencia en la utilización de los recursos (la cual planea cambiar) y su alta dependencia de su creador.

En el último año, *Ether* alcanzó su mayor cotización el 08 de noviembre de 2021 con $4532,07 y un mínimo de $1422,08 el 27 de julio de 2021, siendo de $2944,94 al 13 de febrero de 2022 (figura 5).

Figura 5

Valor del ether (periodo: 2016-2023) (expresado en dólares)



Nota: Tomado de https://coinmarketcap.com/currencies/ethereum/

Ripple (XRP)

Se trata de un software encriptado que posse su propia criptomoneda llamada Ripple (XRP) la misma que ha ganado popularidad en los últimos años debido a su enfoque en el sector financiero. A diferencia de otras criptomonedas, que a menudo se ven como una alternativa a las monedas tradicionales, Ripple se enfoca en proporcionar soluciones de pago más rápidas y eficientes para las instituciones financieras. Sus creadores sostienen que es un sistema seguro que da confianza a sus usuarios. La tecnología de Ripple permite transferir fondos en tiempo real, lo que puede reducir significativamente los costos y los tiempos de transacción en comparación con los sistemas tradicionales. Además, Ripple ha establecido asociaciones con varias instituciones financieras importantes en todo el mundo, lo que ha ayudado a aumentar su legitimidad y su adopción en el sector financiero. Sin embargo, Ripple también ha sido objeto de controversias en el pasado debido a su relación con los bancos y su estructura centralizada, lo que ha llevado a algunos a cuestionar su naturaleza descentralizada y su verdadero valor como criptomoneda. Cabe recalcar que, RIPPLE se creó con la finalidad de mejorar las transferencias monetarias en las entidades bancarias, disminuir los costos de servicio y aumentar la velocidad de los pagos internacionales (López Gómez-Cadiñanos, 2021).

Figura 6

Logotipo de Ripple y símbolo de XRP



Nota: Tomado de http://bit.ly/3kDA5BP

Según Ciaian *et al.* (2018), su proyecto consta de tres pilares: la empresa principal Ripple Labs, la red de pago que ofrece sus servicios a las entidades bancarias y su propio *token XRP. Ripple* es aceptado por parte de las entidades bancarias, muchas de las cuales están optando por la tecnología de este software para reducir los tiempos de las operaciones, ya que es capaz de procesar 1500 transacciones simultáneamente. Presta servicios de transacción rápida internacional, facilitando los procesos de pagos globales a entidades financieras y comerciales, ofreciendo además conectividad, velocidad, certeza de rastreabilidad y bajos costos (Schwartz *et al.,* 2014, citados por Fernández *et al.*, 2021). También provee liquidez para transacciones que requieran carta de crédito.

Algunas de sus características son:

- Funcionalidad: opera como un método de pagos que puede ser utilizado por el sistema financiero tradicional, el cual permite a diferentes entidades financieras realizar transacciones de dinero a mayor velocidad y menores costos (Fernández *et al.*, 2021).
- Criptoactivo propio: *XRP*.
- Mecanismo de generación de bloques: cuenta con el Algoritmo de Consenso del Protocolo Ripple (*RPCA*, por sus siglas en inglés).
- Cantidad máxima: está fija en 100 mil millones, con un crecimiento de la oferta indefinido. En principio se lanza a circulación la mitad de todas las unidades, mientras *opencoin* retiene el resto y se emiten a medida que se van desarrollando los algoritmos que la conforma (Fernández *et al.*, 2021).
- Velocidad de las transacciones: la creación de bloques tiene una duración entre tres y cinco segundos (Fernández *et al.*, 2021).

Entre sus principales ventajas se encuentra su aceptación y adopción por parte de entidades del sistema financiero tradicional y su eficiencia en hardware y uso de la energía se refiere. Entre sus desventajas está el ser de fuente cerrada, rompiendo con el principio de red distribuida y de ruptura con la existencia de intermediarios.

Al revisar el valor del *XRP* durante el periodo comprendido entre febrero 2021 y febrero 2022 (figura 7), se puede observar que su mayor cotización se alcanzó el 13 de abril de 2021 con un monto de $1837 y la menor el 27 de febrero de 2021 con $0,416. Para el 13 de febrero de 2022, su valor de $ 0,806.

Figura 7

Valor del XRP (periodo: febrero 2021-febrero 2022) (expresado en dólares)



Nota: Tomado de https://coinmarketcap.com/currencies/xrp/

Litecoin (LTC, Ł)

Según Melodía (2020), *litecoin* es una criptomoneda que fue creada en 2011 como alternativa al *bitcoin,* la cual sustenta sus operaciones en una red distribuida P2P y un software de código abierto publicado con licencia MIT (figura 8).

Figura 8
Logotipo de Litecoin



Nota: Tomado de https://upload.wikimedia.org/wikipedia/commons/e/e3/Litecoin_Logo.jpg

Según Rus (2021), entre algunas de sus características destacan:

- Es una alternativa que resulta ser atractiva para los inversores debido a que es más económica que el Bitcoin.
- Criptoactivo propio: *LTC*.
- Su mecanismo de generación de bloques es mucho más rápido que Bitcoin.
- Su peso medio es bajo.
- Su algoritmo incluye un cifrado de lado a lado.
- Permite una división de hasta en ocho decimales.

Esta ha activado el *SegWit*, una actualización que aumenta el tamaño de cada bloque, lo que permite contar con una mayor velocidad al momento de realizar el procesamiento de las transacciones, además de la posibilidad de efectuar transacciones *inter-blockchains*, última versión con la cual se dispondrá próximamente.

Los ordenadores que conforman la red y participan en el minado de LTC se agrupan en pools con la finalidad de resolver de manera conjunta un problema criptográfico. Cuando alguno lo resuelve y se verifica

el resultado en la red, *litecoin* otorga una recompensa que se reparte entre todos los participantes, aumentando la probabilidad de recibir *coins* durante los procesos de minado (Vázquez, 2019).

En el último año, LTC logró su mayor cotización el 08 de mayo de 2021 alcanzando los $ 388,28 por unidad y la mínima de $ 106,95 el 26 de enero de 2022, registrando un valor de $126,26 al 13 de febrero de 2022 (figura 9).

Figura 9

Valor del litecoin (periodo: 2013-2023) (expresado en dólares)



Nota: Tomado de https://coinmarketcap.com/currencies/litecoin/

Cardano (ADA)

Se trata de una plataforma y protocolo *blockchain* que entró en el mercado en 2017, luego de dos años de desarrollo por el *Exchange Bittrex*. Cardano está conformado por tres organizaciones para abordar el proyecto, a saber, *Cardano-Foundation*, las empresas IOHK y Emurgo (Morales, 2021).

Figura 10
Logotipo de Cardano



Nota: Tomado de http://bit.ly/3SQ5VYr

Esta criptomoneda se crea con el fin de solucionar las debilidades técnicas que aún persisten en las *blockchain*, estableciéndose que el proyecto se desarrollaría a través de investigaciones académicas sometidas a revisión entre pares (*peers*). Su código se ha reescrito a un nuevo lenguaje de programación (*Haskell*), el cual se considera otorga mayor seguridad y confiabilidad (McCoy, 2019).

Según Otero (2022), entre algunas de sus características destacan:

- Criptoactivo propio: *ADA*.
- Facilita la generación de contratos inteligentes (*Smart contracts*).
- Su funcionamiento es más amigable con el medioambiente en comparación de otras criptomonedas.
- Los usuarios pueden proponer cambios y mejoras a su ecosistema.
- Pertenece a una blockchain de tercera generación.

En la actualidad, *Cardano* trabaja en el desarrollo de una plataforma que permita la interacción entre los protocolos de las criptomonedas

y los de la comunidad financiera, con la finalidad de lograr trabajar y negociar sin necesidad de recurrir al dinero fiduciario, garantizando la legitimidad de las operaciones.

Durante el periodo comprendido entre febrero de 2021 y febrero 2022, *ADA* alcanzó su máxima cotización el 02 de julio de 2021 al llegar a los $ 2,968 por unidad y su mínima de $ 0,8605 el 14 de febrero de 2021, registrando para el 13 de febrero de 2022 un valor de $ 1,05 (figura 11).

Figura 11

Valor del ADA (periodo: 2017-2023) (expresado en dólares)



Nota: Tomado de https://coinmarketcap.com/currencies/cardano/

Criptomonedas estables (stable coins)

Como respuesta a la alta volatilidad evidenciada en las cotizaciones de las criptomonedas, se han desarrollado las criptomonedas estables o *stable coins*, las cuales han sido concebidas para su utilización como medio de pago dotadas de estabilidad a través de mecanismos basados en algoritmos y su vinculación a un colateral, en el caso de *tether* que incorpora una unidad de moneda *fiat* donde 1 *tether* siempre equivaldrá a

1 USD o a su par fiduciario (como USD, EUR o Yen), razón por la cual lo encontrarás representado de la siguiente manera: USD₮, EUR₮, JPY₮ o USDt, EURt, JPYt, según su moneda de partida (Rodríguez Quejido, 2019).

Figura 12

Valor del tether (periodo: 2015-2023) (expresado en dólares)



Nota: Tomado de https://coinmarketcap.com/currencies/tether/

Otra muestra de este tipo de criptomonedas es el caso de JP MORGAN, que anunció una moneda con tales características con la finalidad de utilizarla en una plataforma *blockchain* desarrollada en *quorum*, la cual es una adaptación de *ethereum* al ámbito financiero. Con esta se pretende que se utilice por otras entidades para servicios de pago, no así de forma directa por clientes finales (Rodríguez Quejido, 2019).

Otra forma de colateralizar una *stable coin* es el establecimiento de creación de una cesta de diferentes divisas, tal como lo propone la criptomoneda “libra” que proyecta emitir Facebook (Rodríguez Quejido, 2019). Presentada en 2019 y creada por 27 socios incluidos algunos como Uber, Sportify, Visa o Mastercard. Basados en la tecnología *blockchain*,

estaría respaldada por activos financieros con el fin de intentar evitar la volatilidad y estando su valor vinculado a monedas estables y reguladas ya existentes, como el dólar estadounidense, el euro o la libra esterlina. Contando con la capacidad de Facebook para alcanzar un gran número de usuarios a través de las aplicaciones de WhatsApp, Messenger e Instagram. Además, ha creado su propia cartera digital para almacenar el dinero, Calibra, con la cual no sería necesaria una cuenta corriente en un banco. (López Gómez-Cadiñanos, 2021).

Inicialmente concebida como una moneda global, ha evolucionado en una *stable coin*, ante la oposición de gobiernos y entidades financieras debido a los grandes riesgos que implicaría para el sistema financiero mundial, en particular dados los serios cuestionamientos hacia Facebook por el uso indebido de los datos personales de sus usuarios, situación que ha producido la salida de algunos de sus socios.

Monedas meme

Se trata de criptomonedas inspiradas en memes o chistes en el internet y las redes sociales. En este sentido, se ubica el primer lanzamiento en 2013 con la creación de *dogecoin*, como parodia del meme *Doge,* un perro Shiba Inu japonés. Este tipo de moneda suele presentar un suministro muy grande o ilimitado, carece de mecanismos de minado y tienda a ser muy volátil, dependiendo del apoyo (o no) de las comunidades en línea (Binance Academy, 2021c).

Su popularidad ha ido de la mano de las expectativas de ganancias ante un alza especulativa, en virtud de su bajo precio, así como el apoyo de sus respectivas comunidades. Sin embargo, representan un alto riesgo financiero, ya que solo pocas de estas monedas han sido creadas sobre la base de la tecnología de las principales criptomonedas, además de ser más especulativas y con ciclo de vida más corta. Sin dejar de considerar aquellas que se crean con la intención de aprovechar las expectativas para incurrir en estafas y prácticas oportunistas.

Capítulo 3

Bitcoin

Funcionamiento y características

Su creación se ubica en 2008, cuando bajo el seudónimo de Satoshi Nakamoto se hace público su propuesta y diseño. El 3 de enero de 2009 se creó el *bloque génesis* (primer bloque de *bitcoin*). El *bitcoin* es la primera criptomoneda que por su naturaleza virtual y su base en la tecnología *blockchain* cuenta entre sus características que pueden pasar por alto las restricciones locales para realizar transferencias internacionales por transmitirse directamente a la red *peer-to-pe*er sin la participación de intermediarios (bancos o instituciones centralizadas), menores costos de transacción y con un sistema de validación de pagos descentralizado (Nakamoto, 2008; Fernández *et al.*, 2021; Binance Academy, 2020d; López Gómez-Cadiñanos, 2021).

Figura 13
Logotipo de Bitcoin



Nota: Tomado de http://bit.ly/3mpLNAn

Recordando que en ese momento se presentó la crisis financiera de los grandes bancos en Estados Unidos, se propuso como respuesta a las necesidades de seguridad y garantía de las transacciones virtuales, en virtud del alto riesgo que tienen las partes debido a las probabilidades de fraude en el cual su institución de confianza (sistema financiero internacional) no asumiría la totalidad de la pérdida. Además, en el documento oficial de creación del *bitcoin* se asegura que más que una institución de confianza se requieren servidores con sellos que generen pruebas computacionales de las transacciones que protejan al vendedor y comprador (Nakamoto, 2008).

El *bitcoin* es considerado como el primer criptoactivo y conserva la característica de no ser confiscable, así como de no ser censurable.

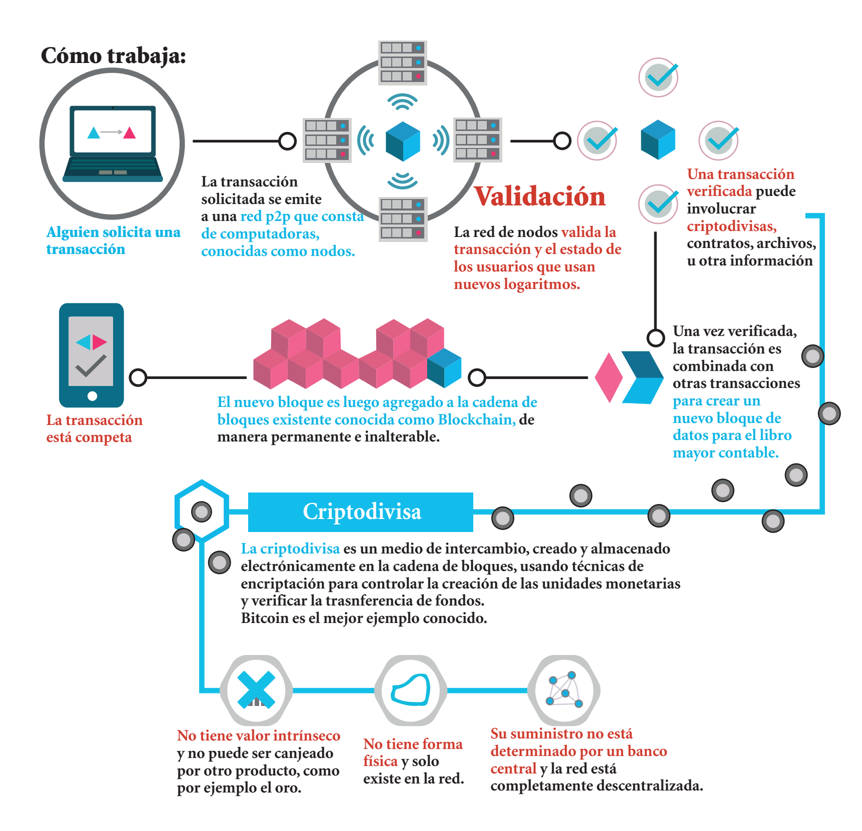
El *bitcoin* tiene una oferta finita de 21 millones de unidades, las cuales se crean a través de la minería asociada a la verificación y validación de las operaciones, su inclusión en el bloque, hasta su incorporación a la *blockchain,* proceso que está programado para que tenga una duración de aproximadamente 10 minutos. Tal validación se realiza a través de algoritmos de consenso PoW. Al culminar exitosamente, se genera la llamada recompensa de bloque (*block reward*) que constituye la forma de generar *Bitcoins* y las comisiones de las transacciones realizadas (figura 14) (Nakamoto, 2008; Fernández *et al.,* 2021; Binance Academy, 2020d; López Gómez-Cadiñanos, 2021).

La validación a través del sistema de prueba de trabajo (PoW), requiere que los mineros realicen actividades de verificación y añadan bloques de información, para lo que es necesaria la resolución de logaritmos matemáticos de alta complejidad, haciendo falta solo el conocimiento sino de capacidad financiera para contar con los equipos adecuados, cubrir el alto gasto energético y mantener la seguridad del sistema las 24 horas del día. Este modelo de PoW contribuye a la seguridad y validez del sistema; sin embargo, produce una alta ineficiencia en el uso de los recursos y un entorno hostil tomando en cuenta que la recompensa solamente la obtiene el minero que logre efectivamente

incluir el bloque en la cadena (Parra *et al.*, 2019; Fernández *et al.*, 2021; Binance Academy, 2020d).

Figura 14

Proceso de minado de bitcoin



Nota: Tomado de Tecno Global Solution (2020).

De manera resumida, una prueba de trabajo funciona de la siguiente manera: cuando un nodo de la red desea ejecutar una transacción con *bitcoins*, lo debe comunicar a todos los demás ordenadores conectados a la red. Cada uno de los computadores que recibe la ins-

trucción debe verificar la validez de la transacción, para lo cual debe cumplir con todas las reglas acordadas por todos los participantes. El resultado también debe ser comunicado a todos los nodos de la red. Este proceso se repite de manera indefinida con el objetivo de que la totalidad de la información sobre las transacciones sea difundida a todos los integrantes de la red.

Vale la pena mencionar que dentro de la red de bitcoin se pueden distinguir dos tipos de nodos:

- Nodos completos: contienen toda la información histórica de todas las transacciones ejecutadas en la red.
- Nodos mineros: son nodos completos pero que además tienen la capacidad de introducir bloques nuevos en la red de *bitcoin*.

Según diversos autores (Fernández *et al.*, 2021: Bolaños *et al.*, 2019; Romo Conde, 2021; Binance Academy, 2018a, 2020d), entre algunas de las características de la prueba de trabajo destacan:

- Funcionalidad: requiere de hardware dotado de alta capacidad de computacional para la resolución de los algoritmos y resguardo de la *blockchain*.
- Criptoactivo propio: *BTC*.
- Mecanismo de generación de bloques: se basa en una red P2P, distribuida, con algoritmo PoW.
- Cantidad máxima: cuenta con una cantidad máxima fija de 21 millones, con generación decreciente a la mitad cada 210 000 bloques.
- Velocidad de las transacciones: los bloques se procesan cada 10 minutos.

Valor del *bitcoin*

Según Ciaian *et al.* (2018), los factores que ha influido en el precio del *bitcoin* son la oferta y demanda del mercado, el interés de los inversionistas, la influencia en el desarrollo de los mercados macrofinancieros en

el mundo y los vínculos que ha ganado con la economía de bienes físicos en la medida que los minoristas empezaron a aceptarla como una forma de pago, aunque no todos usan el mismo método (Pieters y Vivanco, 2017).

El precio del *bitcoin* es un producto de la especulación, junto con las fuerzas de oferta y demanda del mercado; los cuales generan un indicador atractivo para los inversionistas, donde la interacción con el mercado global aumenta la incertidumbre en virtud de la ausencia de respaldo de valor que efectivamente su confianza y disminuya los riesgos de la inversión (Ciaian *et al.,* 2016).

Así, el valor del *bitcoin* está asociado al precio de mercado, marcado por la subjetividad y la especulación, lo que explica su volatilidad. Binance Academy (2021d) señala algunos factores en los cuales se basa este valor:

- Utilidad: se refiere a los beneficios que se derivan de su capacidad para transferir de forma rápida grandes cantidades de valor en todo el mundo, sin requerir de intermediarios. Las comisiones pudieran considerarse grandes cuando se trata de operaciones por montos pequeños.
- Descentralización: debido a la tecnología *blockchain* y su código abierto.
- Distribución: la participación de muchas personas mejora la seguridad de la red, en la medida que se conecten más nodos a la red, más valor tendrá.
- Confianza: la tecnología de *bitcoin* ha demostrado ser muy confiable y segura. Además, su código fuente es abierto y su algoritmo de consenso *Proof of Work* es un mecanismo transparente, verificable y comprobable por sí mismo.
- Escasez: existe un suministro limitado de 21 millones de BTC.
- Seguridad: los ataques maliciosos a la red *bitcoin* requieren contar con la participación de más del 51 % de la potencia minera actual, lo que hace de coordinación a escala mundial sea casi imposible de lograr. De allí que la probabilidad de un ataque exitoso es extremadamente baja y, en caso de ocurrir, duraría muy poco tiempo.

- Reserva de valor: está ganando reputación como alternativa moderna de reserva de valor.

Un aspecto resaltado por Ciaian *et al.* (2016) es la importancia del valor de la información en la formación de precios del *bitcoin*, en virtud de que se trata de un determinante de las decisiones de compra o venta de los participantes y de la volatilidad de su precio. Al momento de su creación, el precio del *bitcoin* era de $0,03/1BTC aproximadamente y a lo largo del año 2010 su precio más alto registrado fue de $0,39. Más reciente, alcanzó su máxima cotización el 07 de noviembre de 2021 al llegar a los $67 549,14 por unidad y su mínima de $ 29 795,55 el 10 de julio de 2021, registrando para el 12 de febrero de 2022 un valor de $ 42 353,74 (figura 15).

Figura 15

Valor del bitcoin (periodo: 2013-2023) (expresado en dólares)



Nota: Tomado de https://coinmarketcap.com/currencies/bitcoin/

Tipos de *bitcoins*

Luego del lanzamiento de la criptomoneda en 2009, se han generado nuevas versiones de *bitcoin* como respuesta de la comunidad a las limitaciones en cuanto a la demanda y el incremento masivo de las transacciones que han sobrepasado el rendimiento de la red, produciendo demoras en el procesamiento de las transacciones y el aumento de las comisiones. Como consecuencia se han producido bifurcaciones, dando lugar al *bitcoin cash* en primera instancia y *bitcoin gold* unos meses después (Domínguez y García, 2018).

- *Bitcoin* (*BTC*): criptomoneda original que da origen a todas las divisas virtuales posteriores.
- *Bitcoin cash* (*BCH*): criptomoneda creada en 2017 a partir del bitcoin con la finalidad de acelerar la velocidad de las transacciones. Desde su salida a los mercados, ha venido cotizando al alza.
- *Bitcoin Gold* (*BTG*): nace en 2017 a partir de otra división más en los bloques de la *blockchain* de *bitcoin*, con el objetivo de mejorar los rendimientos económicos del sistema de recompensas y liberar la red de las grandes compañías que están influyendo de forma negativa en el curso de la moneda.

También se desarrolló la *Lighthing Network* como solución a la escalabilidad, siendo una solución de "capa dos" alejando las transacciones de la *blockchain*, en lugar de registrar todas las transacciones en la *capa base*, se realizan a través de otro protocolo incorporado encima que les permite a los usuarios enviar fondos casi al instante y de forma gratuita, sin restricciones en el rendimiento (Binance Academy, 2020a).

Opciones para la obtención del *bitcoin*

Cuando un usuario desea adquirir criptomonedas, la manera de obtenerlas a través de internet y deben almacenarse en un monedero virtual, aunque ya existe en algunos países la opción de materializarlos en cajeros

automáticos (López Gómez-Cadiñanos, 2021; Binance Academy, 2020d). En general, se cuenta con tres posibilidades para obtenerlas, a saber:

- Minería: los *bitcoins* se obtienen como recompensa, una vez que se logra validar e incorporar un bloque a la cadena, tal como se ha detallado anteriormente.
- Compra: la forma más utilizada es a través de las plataformas *exchange*, las cuales a su vez sirven de monedero digital. No requiere otros intermediarios para concretar las operaciones, por lo que sus costos son mínimos. En tales plataformas es posible comprar, vender o intercambiar criptomonedas. Se pueden comprar con monedas de circulación legal y pagar con tarjeta de crédito o débito, o con otras monedas virtuales.
- Salario en divisas electrónicas: existen empresas en algunos países que pagan el salario de sus empleados en criptomonedas, utilizando el *bitcoin* como referencia.

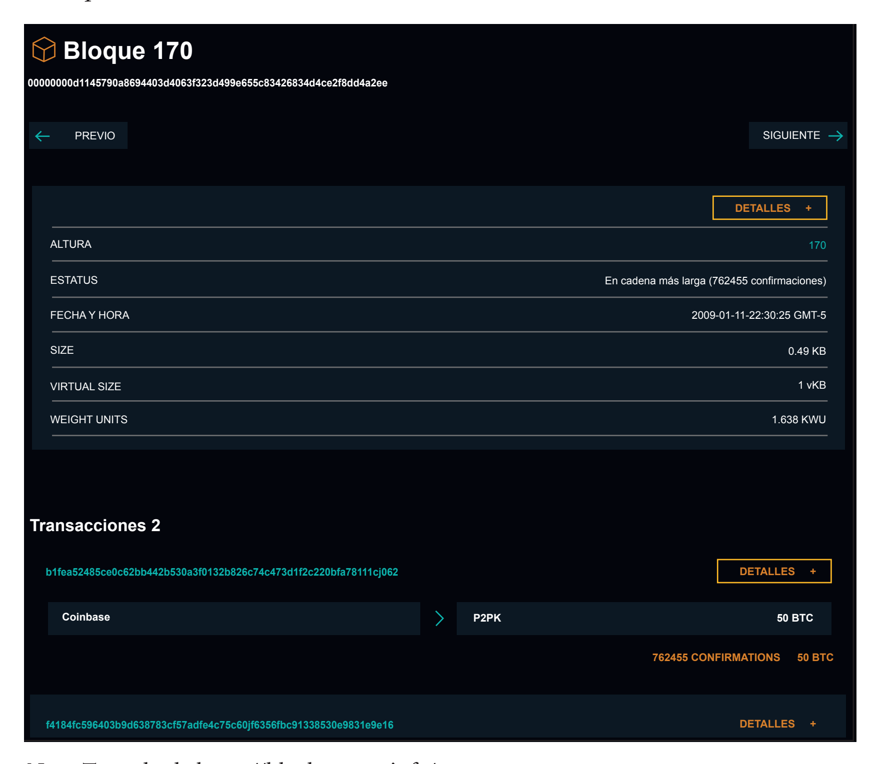
Funcionamiento del *bitcoin*

Como se ha mencionado ya en varias ocasiones, *bitcoin* consiste en una cadena de bloques que se almacena en una base de datos descentralizada; esto requiere que todos los ordenadores que conforman la red trabajen de manera colaborativa y sincronizada, de tal manera que la información almacenada en cada uno de ellos sea una réplica exacta de la información que tienen almacenada los demás ordenadores. Esto se logra mediante un software de código abierto que cada nodo de la red debe ejecutar; este programa realiza la tarea de validar que cada uno de los bloques cumplan con las reglas acordadas por los mineros. En principio, cualquier usuario de un computador puede descargar dicho software e instalarlo para formar parte de la red. De esta manera, todos los miembros de la red validan todos los bloques que transitan por ella, con ello se establece que una transacción es válida o no, si algún nodo de la red no está conforme con el resultado no se da por legítima la validación, caso contrario, cuando todos los nodos validan satisfactoriamente

un bloque se determina a la transacción como legítima; este proceso se conoce como "consenso". Debido a este funcionamiento se dice que este sistema es incorruptible.

Cada transacción puede entenderse como una transferencia electrónica de bitcoins de un usuario A hacia un usuario B. El primer movimiento de esta criptomoneda la realizó Satashi Nakamoto el 11 de enero de 2009, quien transfirió diez *bitcoins* a Hal Finney, lo cual se puede verificar mediante la página https://blockstream.info/ en la figura 16.

Figura 16
Resultado de la transacción realizada utilizando el bloque 170 de la blockchain de bitcoin



Nota: Tomado de https://blockstream.info/

Pero el *bitcoin* no tenía un valor económico dentro del mercado, a pesar de ello, el 22 de mayo de 2010 un profesional informático llamado Laszlo Hanyecs fue el primero en intercambiar *bitcoins* por un producto real, compró dos pizzas a cambio de 10 mil BTC. Si se realizara esta misma compra con el precio actual del *bitcoin* se podría decir que Hanyecs compró las pizzas más caras de la historia.

Sin embargo, no fue sino hasta el 5 de octubre de 2010 que se realizara la primera transacción de compra-venta dándole al *bitcoin* un valor económico de aproximadamente $0.000764 dólares americanos. En aquella ocasión se vendieron 1309 BTC por un dólar estadounidense. El valor máximo histórico que *bitcoin* ha alcanzado fue de aproximadamente $65 000 dólares americanos en noviembre de 2021 (ver figura 17).

Figura 17

Valores históricos del bitcoin en el mercado



Nota. Tomado de https://coinmarketcap.com/currencies/bitcoin/

Existen entonces razones suficientes para considerar que el *bitcoin* fue el primer activo de carácter digital, pues a diferencia de otro tipo

de archivos digitales, las cadenas de bloques de *bitcoin* no pueden ser replicadas digitalmente, siempre tendrán un único dueño y el sistema es prácticamente incorruptible. Para ello la tecnología *bitcoin* utiliza un sistema de criptografía asimétrica (o criptografía de clave pública), el cual consiste en la utilización de dos claves diferentes, una para encriptar el contenido y la otra para desencriptarlo. Una persona, para demostrar que es el auténtico dueño de cierta cantidad de *bitcoins* y transferirla a otra persona, encripta el contenido de su mensaje con su clave privada (es importante que ningún otro usuario tenga acceso a esta clave aparte del dueño) y comparte su clave púbica con todos los demás miembros de la red; de esta manera, cualquier usuario puede confirmar la autenticidad de la clave privada del dueño, pero no podrá modificar el mensaje debido a que para ello necesitaría la clave privada. Las claves públicas también son utilizadas para crear direcciones a las cuales una persona puede recibir *bitcoins*, pero hay que tener presente que el proceso no es reversible, es decir, es imposible determinar una clave pública a partir de una dirección creada con dicha clave.

Ventajas y desventajas del *bitcoin*

Entre sus ventajas, Fernández *et al.* (2021) destacan el hecho de que esta es una criptomoneda y solo se ocupa de transacciones, su buena reputación y su amplia aceptación como medio de pago. Entre las desventajas se encuentran la volatilidad de su precio, los elevados costos de la actividad de minería en cuanto a requerimientos de inversión en *hardware*, la cartelización de mineros dado que la extracción en solitario se hace imposible y solo unas pocas agrupaciones de bits controlan la cadena de bloques, el tiempo de las transacciones (10 min.), la competencia hostil entre los participantes y su innegable ineficiencia debido el elevado consumo de energía con su consecuente impacto medioambiental. Adicionalmente, existen otros riesgos debido a la posibilidad de perder la clave privada de acceso, ya que no existe manera de recuperarla y, en consecuencia, no se puede recuperar los montos correspondientes.

Billeteras o monederos digitales

Una billetera o un monedero (o *wallet* en inglés) "es una herramienta que puedes usar para interactuar con una red *blockchain*" (Binance Academy, 2019b), la cual consiste fundamentalmente en un programa informático que permite el acceso a diferentes cadenas de bloques, de tal forma que se pueda visualizar el balance de la cuenta, así como enviar y recibir dinero. Cada billetera contiene solo las claves públicas y privadas de cada usuario, que le permiten tener acceso a las cadenas de bloques donde las criptomonedas se encuentran "almacenadas" (Leal, 2022).

Funcionamiento de las billeteras digitales

Las billeteras "pueden generar la información necesaria para enviar y recibir criptomonedas a través de transacciones en *blockchain*" (Binance Academy, 2019b), que contiene de uno o más pares de claves públicas y privadas. Además, incluye una dirección, la cual es un identificador alfanumérico generado a partir de las claves pública y privada. Esta dirección es una "ubicación" específica en la cadena de bloques donde se pueden enviar las monedas. Por lo tanto, puedes compartir la dirección con las otras personas con la finalidad de recibir fondos y, en ningún caso, la clave privada. La clave privada otorga acceso a las criptomonedas, sin importar la billetera utilizada.

Tipos de billeteras digitales

Es posible clasificar las billeteras digitales de acuerdo con diferentes criterios, entre los que se pueden mencionar: cantidad de criptomonedas que puede manejar (una o varias), con custodia o sin custodia, tipo de dispositivo utilizado (apps móviles, desktop/software descargable, online, hardware, tarjetas/papel, otros) o conexión a internet, entre otros (Parra *et al.*, 2019; Binance Academy, 2019b, 2020d, 2021d, 2021e). En este punto se presentan los tipos de billeteras digitales según su conexión a internet, a saber:

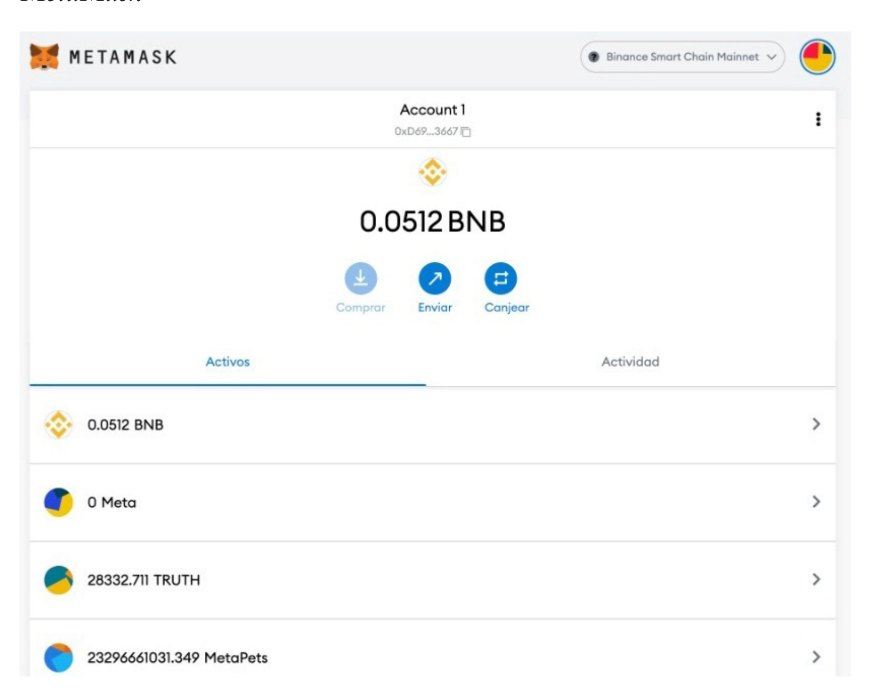
- Billeteras o monederos calientes (*hot wallets*): constituye un *software*, el cual se conecta a internet. Por lo general, es una app móvil o de ordenador de escritorio, a través del cual es posible enviar y recibir monedas. Suelen ser convenientes para realizar pagos, aunque tienen mayor vulnerabilidad ante ataques maliciosos. Como ejemplo de estos monederos se encuentra Trust Wallet y Binance.
- Billeteras o monederos fríos (*cold wallets*): este tipo de monedero no se encuentra expuesta a internet; por lo tanto, son menos susceptibles de ser objeto de ataques maliciosos. Utilizan un medio físico con el fin de almacenar las claves, manteniéndolas fuera del entorno digital, con lo cual son menos vulnerables. Sin embargo, esta misma característica, hace que su utilización sea un poco más engorrosa, pero más recomendable para quienes desean conservar inversiones de largo plazo. Entre estas se cuentan las billeteras de hardware o las de papel.

Billeteras digitales más utilizadas

A continuación se presentan algunas de las billeteras digitales más utilizadas:

- *MetaMask:* fue desarrollada en 2016 por *ConsenSys*. Se trata de una extensión de navegador y una criptobilletera de tipo aplicación móvil compatible con diversas *blockchain* como *Ethereum*, *Polygon*, *Binance Smart Chain (BSC)* y *Binance Chain* (figura 18) (Bit2me Academy, s.f.).
  La extensión de navegador de *MetaMask* permite realizar transacciones e interactuar con contratos inteligentes y aplicaciones descentralizadas (*DApps*) (Binance Academy, 2021f). Esta última brinda a los usuarios acceso seguro a distintos servicios y se pueden utilizar en computadores personales, teléfonos inteligentes o vía *web* (Bit2me Academy, s.f.). También permite la conexión a diferentes *blockchain*, firmar transacciones, gestionar claves públicas y privadas, y cuenta con un servicio de intercambios (*swaps*) que brinda los mejores precios de múltiples *exchanges* descentralizados.

Figura 18
MetaMask



Nota: Tomado de *MetaMask*, https://metamask.io/

- *Trust Wallet:* es una billetera móvil de código abierto disponible para iOS y Android. Es la billetera descentralizada oficial de Binance, y compatible con los ecosistemas *blockchain* de *Ethereum*, *BSC*, *Binance Chain*, entre otros. En ella, el usuario cuenta con acceso completo a sus claves privadas mediante una "frase semilla". La aplicación presenta algunas funcionalidades extra incorporadas, como la compra de criptomonedas a través de tarjeta de crédito o débito, y una billetera para *tokens* no fungibles (NFTs). Además, la versión Android dispone de un navegador para *DApps* (Binance Academy, 2021f). *Trust Wallet* tiene un *token* de tipo "*utility*" y de

gobernanza, llamado *TWT*, el cual permite participar en la toma de decisiones como añadir soporte para nuevas *blockchains* e integrar nuevos *tokens*, y también obtener descuentos en el *DEX* y en la compra de criptomonedas (Binance Academy, 2021e).

- *MathWallet:* es una billetera de criptomonedas de tipo extensión de navegador, y una *app* móvil para dispositivos iOS y Android, compatible con casi 40 *blockchains* diferentes. Fundada por MATH Global Foundation en 2017, ofrece la flexibilidad suficiente para utilizar la misma billetera en distintos dispositivos. Según las necesidades de los usuarios, resulta fácil moverse entre el dispositivo móvil, la extensión del navegador y la billetera de base web (Binance Academy, 2021f).
- *Binance Chain Wallet:* es la billetera de tipo extensión de navegador oficial de Binance, compatible con *Binance Chain*, *BSC* y *Ethereum* (figura 19). Cuenta con una función *Wallet Direct*, la cual es utilidad para usuarios que tienen criptomonedas en el *exchange* de *Binance*, pero ocasionalmente usan *DApps* (Binance Academy, 2021e).
- *SafePal*: se trata de un proveedor de billetera hardware que también ofrece una billetera móvil descentralizada de tipo app. Con una funcionalidad similar a la de *Trust Wallet*, ofrece adicionalmente una sección de finanzas descentralizadas que tiene enlaces a otras plataformas y *DApps* similares, así como un navegador. También cuenta con un *token* de tipo "*utility*", denominado *SFP*, para descuentos y bonificaciones (Binance Academy, 2021f).

Transacciones con criptomonedas

De acuerdo con Parra *et al.* (2019), el proceso de compra de criptoactivos para un usuario común requiere que previamente configure una billetera o monedero digital y abra una cuenta en una plataforma de intercambio. En caso de ser un nuevo usuario en el sistema de criptoactivos, debe adquirirlos a otro usuario vez en la plataforma seleccionada mediante una transferencia electrónica o tarjeta de crédito. Los precios de compra y venta de *bitcoin* incluirán el margen establecido por la pla-

taforma de intercambio, la cual también puede cobrar comisiones por los pagos recibidos y enviados. A través de la tecnología *Blockchain* se verifica y registra la transacción de forma distribuida, en la billetera digita de cada usuario tendrá la información de sus *bitcoins*.

Según Armstrong (2018, citado por Parra *et al.*, 2019), la conexión de las plataformas de intercambio con el sistema financiero hace que estas tiendan a centralizar la estructura del sistema de criptoactivos mientras la adopción de las criptomonedas se masifica. En opinión de Böhme *et al.* (2015), las billeteras digitales propician la centralización de la información de los usuarios como consecuencia de las facilidades que ofrecen para el mantenimiento y utilización de los criptoactivos.

También es posible comprarlas en efectivo entregando físicamente el dinero a otro usuario, quien intercambiará las criptomonedas a través de su monedero digital o adquiriéndolas a través de un cajero electrónico disponible en algunos países. Cuando los usuarios cuentan con criptoactivos, tienen la posibilidad de realizar transacciones para cambiarlos por otras criptomonedas o *tokens*, utilizarlas como medio de pago, a través de una billetera digital.

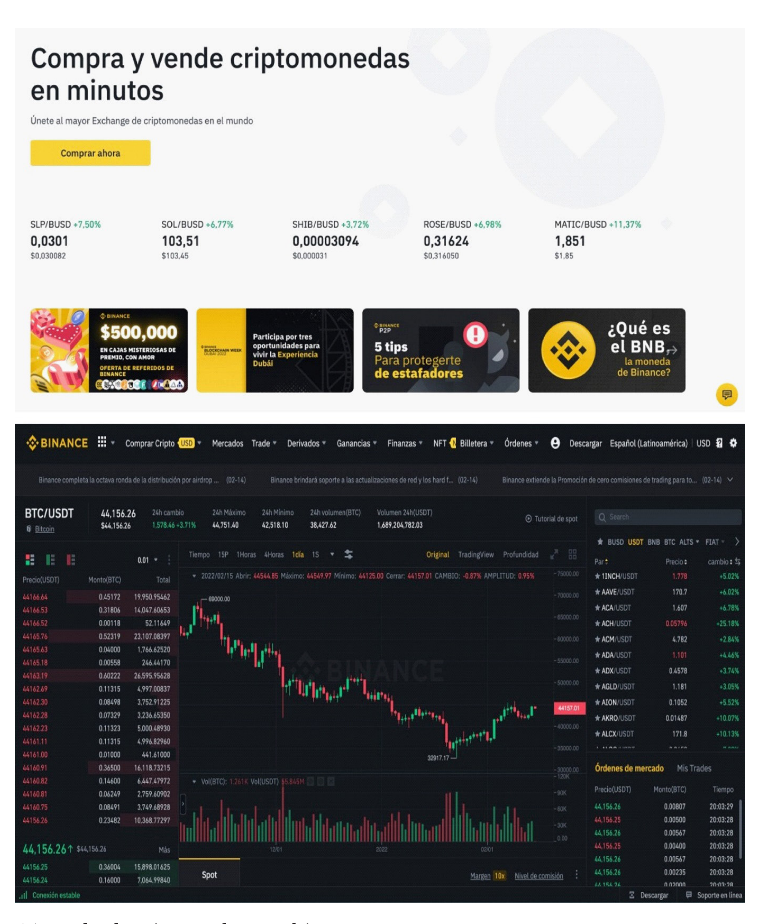
Las criptomonedas han avanzado como forma de pago cuya aceptación ha avanzado paulatinamente. Sin embargo, existen múltiples temas pendientes cuya tendencia pudiera afectar los principios mismos en los que se sustentan. Aspectos como la red distribuida y el seudonimato pueden verse afectadas en la medida que se requieren mayores inversiones en equipos costosos con la suficiente potencia computacional para poder almacenar las bases de datos y procesar rápidamente las transacciones que le permitan a los nodos lograr rendimientos suficientes para recuperar lo invertido, llevando a una merma del número de usuarios en función de su capacidad financiera. Esto hace pensar en la concentración de los nodos en menos manos, aumentando la posibilidad de ataques del 51 %.

La extrema volatilidad de sus precios, susceptibles a situaciones como la opinión de algunas personalidades, instituciones o gobiernos acerca de ellas, es un tema sobre el cual se han hecho algunos esfuerzos aún

insuficientes. La ausencia de terceros para la ejecución de las transacciones es otro tema que está entrando en contradicción. Las billeteras digitales están asumiendo un rol similar a los bancos tradicionales, de custodia e intermediación financiera, el cual es una de las razones principales que dio origen a las criptomonedas.

Figura 19

Binance Chain Wallet



Nota: Tomado de *Binance*. https://binance.com/es

Entendiendo que aún falta mucho por desarrollarse, existen temas importantes sobre los cuales alertar: la ineficiencia excesiva en cuanto a la utilización de los recursos, fraude, lavado de dinero y financiamiento de actividades terroristas, solo por nombrar algunos.

Regulación sobre la tecnología blockchain *en algunos países*

Las aplicaciones de la tecnología *blockchain*, en particular, el *bitcoin*, no tiene una regulación universal que pueda ser aplicada en todos los países, sin embargo, algunos de ellos han aplicado ciertas políticas sobre este nuevo tipo de moneda. A continuación, se citan algunos ejemplos que han sido extraídos de un documento publicado por la Pontificia Universidad Javeriana (s.f.) en el que se aprecia algunos hitos y datos de diferentes países que han tomado la batuta en este tipo de normas y también sobre aquellos que han prohibido el uso de criptoactivos.

Suiza

Su organismo FINMA (Autoridad Supervisora del Mercado Financiero) en 2018 se convirtió en una de las pioneras entidades del mundo en emitir una norma que regula de manera específica al uso de los criptoactivos, reconociendo tres tipos de tokens: *payment tokens* (tokens de pago), *utility tokens* (tokens de utilidad) y *asset token* (títulos valores en blockchain).

Estados Unidos

No ha emitido una política oficial sobre el uso de criptoactivos, pero algunas instancias del gobierno han adoptado los lineamientos de entidades internacionales; no obstante, esto también ha implicado una desorganización provocada por la diversidad de criterios de dichas entidades, por ejemplo: la CFTC (Comisión de Negociación de Futuros de Commodities) considera a los criptoactivos como material tangible que se pueden negociar, la SEC (Comisión de Valores) los define como títulos de valores, la FinCEN (Agencia de Cumplimiento de Delitos Financieros)

los define como dinero, mientras que el Estado de Wyoming considera que los criptoactivos son una propiedad privada.

Malta

Este país es conocido como la "isla blockchain", sobrenombre ganado por la clara regulación que ha adoptado para la regulación de criptoactivos, a través de su Ley de Autoridad de Innovación Digital, Ley de Servicios y Arreglos Tecnológicos Innovadores y su Ley de Activos Financieros Virtuales.

Alemania

Cuenta con una norma que regula el servicio de custodia de criptoactivos, vigente desde el 1 de enero de 2020. Como consecuencia, cualquier entidad financiera o no financiera que ofrezca este servicio lo podrá hacer previa autorización de la BaFin (Autoridad Federal de Supervisión Financiera).

Unión Europea

Hasta marzo de 2020 estuvo recibiendo aportes sobre un documento que especifica algunos aspectos relativos a los criptoactivos, tales como: emisión, intercambio, acceso y transferencia, así como delitos inherentes a esta temática: fraude, ciberataques y manipulación malintencionada.

Catar

Con el fin de precautelar delitos relacionados al lavado de activos y financiamiento de actividades terroristas, este país desde el 2020 prohibió toda actividad relacionada a las criptomonedas; sin embargo, dicha prohibición no considera a los *security tokens*, razón por la cual su uso sería legal.

China

Su gobierno ha estado buscando y probando aplicaciones de la tecnología *Blockchain*, sin embargo, no tienen una regulación específica para ello.

Nueva Zelanda

En 2019, Nueva Zelanda legalizó el pago de los salarios en criptomonedas, algo inédito a nivel mundial. La norma establece que el pago se debe realizar en una criptomoneda que sea fácilmente intercambiable por dinero *fiat* (dinero en efectivo).

España

Su organismo CNMV (Comisión Nacional del Mercado de Valores) ha determinado que la regulación establecida por la Ley de Mercado de Valores debe ser aplicada a los criptoactivos, sean estos *security tokens* o tokens de utilidad. Este criterio se encuentra en constante revisión dada la naturaleza de los criptoactivos.

Colombia

Se encuentra trabajando una ley desde el año 2019 cuyo objetivo principal es "definir los aspectos generales de la operación y funcionamiento de los prestadores de servicios de intercambios de criptoactivos".

Argentina

No dispone de regulación específica, pero su Comisión Nacional de Valores ha manifestado que algunos tokens pueden ser considerados como títulos de valores y aplicaría la regulación existente.

Chile

En 2019 presentó un proyecto de ley que regularía temas relacionados a criptomonedas. Según el Ministro de Hacienda de aquel entonces "la regulación aplicará requerimientos de manera proporcional, regulando según el tipo de servicio prestado y los riesgos que este implica para los usuarios y para el mercado financiero".

Bolivia

Prohibió de forma expresa el uso de criptomoneda mediante un decreto vigente desde el 6 de mayo de 2014.

Brasil

No hay acuerdos ni pronunciamientos oficiales por parte del gobierno sobre esta temática. Han existido posiciones contrarias entre las entidades gubernamentales y la dirigencia del Banco Central de Brasil.

Ecuador

El uso de criptomonedas para realizar actividades de comercio está prohibido desde enero de 2018 mediante un escrito emitido por el Banco Central del Ecuador en el que textualmente dice "el uso de criptomonedas o medios digitales que se utilizan para invertir y realizar transacciones a través de internet no está autorizado en el país". No obstante, las aplicaciones tipo *wallet* funcionan sin inconvenientes.

México

Es de los pocos países latinoamericanos que han decidido regular de alguna manera el uso y comercialización utilizando criptoactivos y tecnología *Blockchain*. Dentro de su Ley Fintech consta una sección dedicada a las criptmonedas reconociéndolas como activos digitales. Según la publicación de la Pontificia Universidad Javeriana dentro de esta temática están involucradas las siguientes entidades mexicanas: Banco de México, la Secretaría de Hacienda y Crédito Público y la Comisión Nacional Bancaria y de Valores.

Perú

Cuenta con procesos regulatorios sobre el dinero electrónico, pero estos no hablan de manera puntal sobre las criptomonedas, por lo tanto, no son reconocidas como divisas legales. A pesar de ello, su uso no está

expresamente prohibido. Algunas instancias gubernamentales han experimentado con procesos basados en tecnología *Blockchain.*

Venezuela

En 2017 inició un proceso de registro y certificación obligatoria de los usuarios que se dedicaban a la minería de criptomonedas. Con este antecedente, en 2018 el gobierno de turno creó dos entidades importantes: por un lado, la Superintendencia Nacional de Criptoactivos y Actividades Conexas que estaría encargada de regular todos los temas conexos relacionados a los criptoactivos, y por otro lado la Tesorería de Criptoactivos de Venezuela que regularía la emisión, custodia, recaudo y distribución de criptoactivos.

Capítulo 4

Token no fungible

Conviene iniciar esta sección describiendo el término *fungibilidad*. Se dice que un objeto es fungible cuando puede ser sustituido en el mercado por otro objeto de similar valor o características, para ello, es necesario que los dos objetos sean comparables entre sí. En otras palabras, la fungibilidad se refiere a una relación que denota equivalencia entre objetos de distinta naturaleza pero que debido a la similitud de su valor pueden ser intercambiables entre sí. El ejemplo más palpable de un objeto fungible es el dinero, pues da exactamente lo mismo tener un billete de cien dólares, dos billetes de cincuenta o cien monedas de un dólar. Un *bitcoin* también es fungible, puede ser intercambiado por su equivalente en fracciones de *bitcoin.*

Un *token no fungible* tiene la característica de no ser igual ni equivalente a otro token no fungible, esta es la principal característica de este tipo de criptoactivos.

Origen de los NFT (*Non-Fungible Token*)

Uno de los primeros usos de la tecnología *blockchain* fuera del ámbito de las criptomonedas, sino en la recreación y el ocio, con impacto significativo, se le adjudica a *Ethereum.* Los *CryptoKitties*, un juego que permite a sus jugadores reunir, criar e intercambiar gatos virtuales con una combinación de propiedades diferentes, como edad, raza o color, haciéndolo único y sin posibilidad de intercambiarse entre sí. Además, son indivisibles.

Los *CryptoKitties* lograron congestionar la plataforma de *Etherum* a finales de 2017. Se estima que representó un 25 % del tráfico en diciembre de ese año, llegando a venderse algunas de las unidades más raras en cientos de miles de dólares (*Binance Academy*, 2021e).

Concepto de NFT

De acuerdo con Binance Academy (2020b, 2021e), un *Token* No Fungible (NFT) también denominado criptocoleccionable, consiste en un tipo de *token* criptográfico en una *blockchain*, el cual representa un activo único, es decir, una criptomoneda que representa algo único, susceptible de ser coleccionado y sin posibilidad de ser replicado. Estos activos pueden ser totalmente digitales o versiones tokenizadas de activos existentes en el mundo real. En virtud de que los NFT no son intercambiables entre sí, es posible utilizarlos como prueba de autenticidad y propiedad en el ámbito del entorno digital.

Se trata de activos digitales únicos, ya que cada uno cuenta con un identificador que lo diferencia de los demás, incluso cuando se refiera a una serie limitada donde todos sean iguales debido a que cada una contará con su propia identificación a través de su código. Esto representa su característica de "No Fungible". Aun cuando se llegue a descargar la imagen o coleccionable asociado al NFT, no implica su propiedad real o autenticidad del mismo

Aspectos relevantes de los NFT

A partir de lo señalado por Binance Academy (2021e), es posible puntualizar los siguientes aspectos en relación a los NFT:

- Representación en NFT: pueden ser coleccionables digitales, obras de arte físicas, obras de arte digitales, canciones, *gifs*, vídeos, coleccionables de videojuegos, todos se pueden representar mediante NFT. El criptoarte y los NFT no se circunscriben a un único formato, así que no hay límites en lo relativo a creatividad aplicada a tu nuevo NFT.
- Billeteras digitales: es importante constatar que la billetera digital compatible con la *blockchain* en la que se cree el *token*. Se recomienda utilizar *MetaMask* o *Trust Wallet*, debido a su compatibilidad con una gran variedad de *blockchains*.

- *Blockchain:* existen muchas compatibles con los NFT, por lo que la selección dependerá de la preferencia personal, costos y velocidad de la transacción. En su mayoría se encuentran en *Ethereum* o *Binance Smart Chain.*
- Plataforma: la elección de la plataforma a utilizar para acuñar los NFT está determinada por motivos personales y la *blockchain* que se desea utilizar. Entre las más recomendadas por su facilidad se encuentran *BakerySwap, Juggerworld* y *Treasureland. BakerySwap* tiene el principal mercado de NFT, siendo una buena opción para quienes deseen vender sus NFT luego de acuñarlos. *Treasureland* permite la acuñación gratuita de los NFT. *OpenSea* o *Rarible* son de las más populares cuando se trata de incluirlas en *Ethereum.*

Usos de los NFT

Por tratarse de que la creación de escasez digital de activos es una tecnología en pleno desarrollo, aún no se ha determinado el alcance de las posibles aplicaciones en los distintos ámbitos, incluso más allá de los coleccionables (Binance Academy, 2021b, 2021e, 2021f). En consecuencia, basados en la experiencia acumulada se puntualizan sus principales usos:

- NFT de arte: la verificación de autenticidad y propiedad digital que otorgan los NFT representan la mayor parte del valor del arte cripto. Cuando se trata de NFT, el valor no necesariamente se relaciona con la obra de arte adjunta, ya que en ocasiones lo más importante es demostrar la propiedad de ese activo. Este es uno de los usos de NFT más populares en la actualidad.
- NFT coleccionables: existe una demanda masiva de coleccionables digitales y representan una significativa proporción de las ventas de NFT. Estos *tokens* crean la cualidad de coleccionable en el ámbito digital, pudiéndose asimilar a versión digital de un autógrafo firmado. Dadas sus características, es frecuente encontrar NFT de artes y, a la vez, coleccionables.

- Finanzas de los NFT: en las finanzas descentralizadas, los NFT también brindan beneficios financieros. Algunos ofrecen un modelo *staking* de NFT, en el que un usuario puede depositar a largo plazo un par de *tokens* durante un período determinado y recibir NFT como retribución, acceso posterior o para su uso en un mercado secundario en función de los beneficios que otorgan.
- NFT de juegos: cuentan con una gran demanda de artículos únicos que se pueden comerciar, intercambiar, comprar y vender, donde su precio depende de su rareza, y los jugadores ya están familiarizados con la idea de artículos digitales valiosos. Las microtransacciones y las compras en el juego se ha transformado en una industria de miles de millones de dólares que aún no ha aprovechado al máximo los NFT y la tecnología *blockchain*. Los *tokens* para videojuegos combinan elementos de arte, coleccionabilidad y utilidad para los jugadores.
- NFT de música: se puede adjuntar un NFT para crear piezas musicales coleccionables. Otras alternativas están en las plataformas de transmisión basadas en *blockchain* y venta de regalías NFT.
- NFT de activos del mundo real: se presenta como una oportunidad para vincular activos físicos con NFT, permitiendo la digitalización de la forma como se demuestra la propiedad en la *blockchain*. Sin embargo, los aspectos jurídicos de operaciones compra-venta de activos como los inmuebles, son inciertos. Cuando se trata de artículos más pequeños, como joyas, un NFT puede ayudar a demostrar la propiedad legítima al revenderlos e integrarse con una billetera digital fría.
- NFT de logística: sus aplicaciones pueden realizar aportes importantes en la trazabilidad de los productos, desde su origen hasta el cliente final, incluyendo la procedencia de las materias primas, mano de obra, especificaciones, entre otros aspectos. Tales posibilidades requieren que toda la cadena de suministro utilice la misma infraestructura.

Creación de un NFT

El procedimiento específico a seguir en la creación de NFT depende de la plataforma seleccionada. En general, se requiere contar con las criptomonedas necesarias para cubrir los montos de las comisiones de creación (*minting fee*), a excepción de aquellas que sean gratuitas, y el archivo digital del elemento (imágenes, audios, videos, *gifts*, otros) a convertir en NFT, al cual se debe agregar los datos y descripciones al momento registrarlo, además de la declaración antiplagio. De igual manera, se define si se trata de NFT individuales o una colección conformada por un grupo de *tokens* (Binance Academy, 2020b, 2021e).

NFT más populares

Cada día se surgen nuevos proyectos de NFT, relacionados con juegos, obras de arte, premios, sellos postales, tarjetas, música, activos físicos, entre otros. A continuación, se listan algunos calificados por *Binance Academy* (2021e) como de los más populares:

- *Decentraland*: consiste en un mundo de realidad virtual descentralizado, en cual los jugadores pueden tener e intercambiar parcelas de tierra virtual, así como otros NFT del juego. *Cryptovoxels* es un juego similar en el que los jugadores construyen, desarrollan e intercambian propiedades virtuales.
- *Alchemy Toys*: es un juego donde los jugadores reúnen juguetes con números de serie únicos representados por NFT, pueden combinarlos para generar otros de mayor nivel o sacrificarlos (quemarlos) para ofrendarlos a los dioses. Tales juguetes son intercambiables, añadiendo un componente financiero y de mercado al juego. Para ganar se debe reunir la totalidad de los 127 juguetes y sacrificarlos. El primer jugador que lo logra en cada ronda, obtiene una fracción del tesoro, la cual se paga en criptomoneda.
- *PancakeSwap*: en este proyecto se realizan sorteos y competencias para los usuarios de la plataforma, donde se reparten conejitos

coleccionables. Algunos son decorativos y otros son intercambiables por *CAKE*, el *token* nativo de esta plataforma.

- *Gods Unchained*: juego digital de cartas únicas coleccionables en forma de NFT en la *blockchain*, donde los jugadores tienen la posibilidad de poseerlas e intercambiarlas con el mismo grado de propiedad como las cartas físicas.
- *CryptoPunks*: se trata de obras de arte digitales coleccionables, donde cada una representa un personaje NFT único en estilo 8 *bits*. Desde su lanzamiento, se venderían por millones de dólares e inspirarían gran cantidad de otros proyectos similares de todo el mundo.
- *My Crypto Heroes*: juego de roles multijugador, donde los jugadores pueden aumentar el nivel de una serie de héroes históricos mediante misiones y batallas. Los héroes e ítems se emiten como NFT en la *blockchain* de *Ethereum*.
- *Coleccionables de Binance y NFT*: *Binance* regala NFT en sorteos especiales y a los usuarios según su actividad en la plataforma. Estos son coleccionables e intercambiables. También, esta plataforma ha creado *Binance Collectibles* (coleccionables) emitidos en colaboración con Enjin, los cuales se entregan como premios por participar en sorteos a través de su cuenta en *Twitter*.
- *Crypto Stamps*: son sellos emitidos por el servicio postal austríaco utilizados para el transporte de correo como cualquier otro tipo de sello. También se guardan como imágenes digitales en la *blockchain* de *Ethereum*, convirtiéndolos en coleccionables digitales intercambiables.

En otras palabras, la dinámica más visible de los NFT en la actualidad está en los juegos, donde sus funcionalidades dentro los propios juegos, así como el atractivo de coleccionarlos e intercambiarlos están conformando un mercado cada vez más valioso, permitiendo generar ingresos a los jugadores. No obstante, sus aplicaciones en otras áreas, como elemento de certificación de autenticidad, propiedad y trazabilidad de activos de toda naturaleza, continúa en desarrollo.

Capítulo 5
Metaverso

Concepto o definición de metaverso

Desde el punto de vista etimológico, la palabra metaverso es un acrónimo de metauniverso, el cual proviene a su vez del griego *meta* (más allá) y del latín *universus* (total, todo lo que lo rodea). La introducción del término por primera vez se ubica en el año 1992 y se le atribuye al escritor estadounidense Neal Stephenson, cuando la utilizó en su novela de ciencia ficción "*Snow Crash*" donde describe un espacio virtual en tres dimensiones (3D), colectivo y convergente donde los humanos interactuaban con sus representaciones virtuales (avatares) que recorren el planeta a pie o en vehículo (Huidobro, 2021; Orellana, 2022; *Binance Academy*, 2021g, 2021h).

Al integrar los planteamientos de autores como Huidobro (2021), Orellana (2022) y Binance Academy (2021g), el metaverso es un entorno o un universo virtual inmersivo que replica al mundo físico y en el que se puede interactuar con otras personas, objetos y espacios, donde los seres humanos interactúan social y económicamente a través de sus avatares en un ciberespacio, el cual actúa como una "metáfora del mundo real", un mundo ficticio, donde existe una realidad similar a la vida real, pero sin las limitaciones físicas, económicas o de otra naturaleza.

Según Alex Rayón, vicerrector de Relaciones Internacionales y Transformación Digital de la Universidad de Deusto, citado por Huidobro (2021), "es más la definición de un momento que de un espacio. Será un momento en la historia donde será indistinguible el mundo digital y el físico. Los momentos de nuestra vida (ir a trabajar, comer con amigos

o ir al cine, por ejemplo) serán indistinguibles en el plano físico y el virtual" (figura 20).

En 2013 se registra el auge de este concepto con el videojuego *Second Life*, de acceso gratuito, en el cual 70 millones de usuarios llegaron a desarrollar actividades, socializan, ganan dinero y compran. Este permite a sus usuarios vivir una vida paralela a través de avatares personalizados. En la actualidad, este juego cuenta solo con un millón de cuentas activas (Huidobro, 2021).

Como otro ejemplo en esta idea de realidad virtual, en el 2020 se lanza la plataforma *Decentraland*, donde unos 60 millones de usuarios alrededor del mundo pueden comprar parcelas de tierra, construir y monetizarlas. Así mismo, se presenta *Roblox*, un juego donde casi 200 millones de usuarios tienen la posibilidad de crear sus propios juegos y utilizan sus avatares para participar en los construidos por otros (Huidobro, 2021).

Figura 20
Personas en experiencias de realidad virtual



Nota. Tomado de Huidobro (2021). Imagen de Lucrezia Carnelos.

Empresas que impulsan el metaverso

Aunque pudiera pensarse que el concepto de metaverso apareció en 2021 con el anuncio de Facebook, ciertamente existen compañías que han venido trabajando en este concepto durante las dos últimas décadas, las cuales han desarrollado tanto software como hardware, cascos y lentes que han sido clave para lograr la vinculación entre el mundo real y el mundo virtual (Orellana, 2022).

En tal sentido, a continuación se presentan las empresas que están desarrollando los proyectos de mayor relevancia en la actualidad:

Google

Esta compañía cuenta con experiencia en realidad aumentada y realidad virtual, que se ha visto reflejada en productos como *Google Glass* y su herramienta de videoconferencias holográficas *Project Starline*. Según Binance Academy (2021j) sus esfuerzos actuales están orientados a la conexión a través de avatares aumentados que permitan la combinación del mundo digital y el físico.

Facebook (Meta)

Desde 2014, con la adquisición de la empresa de gafas de realidad virtual *Oculus VR*, Facebook ha venido desarrollando iniciativas orientadas hacia este tema, cambiando incluso su nombre a Meta en 2021, la cual integra Facebook, Instagram, WhatsApp y Oculus VR (Orellana, 2022; Huidobro, 2021; Binance Academy, 2021j). Entre algunos de los proyectos orientados por la visión de realidad y mundo virtual, se encuentran:

- *Facebook Horizon:* un videojuego en línea que permite a los usuarios la creación de avatares y la interactuación con objetos gracias a los lentes VR.
- *Horizon Workrooms*: consiste en una herramienta para el trabajo.
- *Infinite Office*: espacio que permite a los usuarios crear su lugar de trabajo ideal, mediante la utilización de realidad virtual.

- Mensajería VR: permite conectar a los usuarios de una forma inmersiva.
- Proyecto Cambria: son auriculares VR compatibles con el mundo de realidad virtual *Oculus Quest.*
- *Horizon Marketplace:* constituye un lugar donde compradores, vendedores y creadores pueden intercambiar bienes digitales.
- Libra: proyecto de criptomoneda respaldada por un grupo de socios, la cual se encuentra aún en desarrollo.

Sin dejar de lado los señalamientos del CEO de la empresa, Mark Zuckerberg, quien ha destacado la importancia de los *tokens* no fungibles (NFT), las criptomonedas y las *blockchains* en la construcción del metaverso (Binance Academy, 2021k).

Microsoft

Desde 2021, la empresa incorporó a su oferta el *Microsoft Mesh*, un software de realidad mixta que permite conectarse de forma virtual, donde según Microsoft esta app facilita “la presencia y las experiencias compartidas desde cualquier lugar, en cualquier dispositivo”. Además, cuenta con sus lentes *HoloLens 2* como uno de sus elementos fundamentales y con *AltspaceVR*, una plataforma social de realidad virtual adquirida por *Microsoft* en 2017 (Orellana, 2022; Binance Academy, 2021j).

Para este 2022, se espera el lanzamiento del *software Mesh for Teams,* como complemento de *Mesh* y enmarcado en la tendencia de trabajo remoto acentuado durante la pandemia, el cual se espera esté disponible en dispositivos convencionales y equipos de realidad virtual con la finalidad de crear una “experiencia de oficina virtual duradera” (Binance Academy, 2021k). Para ello, se podrá hacer uso de un avatar creado como identidad digital, quien podrá explorar áreas virtuales y espacios del mundo digital (Orellana, 2022; Huidobro, 2021; Binance Academy, 2021j).

Binance

Esta ofrece la infraestructura necesaria para apoyar los nuevos sistemas y procesos financieros, mejorando la interoperabilidad entre distintos ecosistemas que se están desarrollando en el metaverso, debido a la importancia de las criptomonedas y *blockchain*. Así, la plataforma de mercado de *Binance* NFT provee a compradores y vendedores la posibilidad de intercambiar activos digitales de tipo NFT de múltiples *blockchains*, lo que ayuda a mejorar la interoperabilidad entre distintos ecosistemas del metaverso (Binance Academy, 2021j).

Epic Games

Inicialmente como un simple juego, se ha convertido en una de las plataformas más desarrolladas del metaverso, con más de 350 millones de jugadores. Cuenta con algunos de los videojuegos más populares *Fortnite*, *Minecraft* o *Roblox* debido a que permiten la construcción de mundos virtuales. Los eventos virtuales incluyen una gran variedad de celebridades, marcas y colaboraciones para la realización de ceremonias de premios y conciertos (Orellana, 2022; Binance Academy, 2021j).

Tencent

Posicionada como una de las más importantes vendedoras de videojuegos en el mundo y propietaria de las redes sociales y plataformas de mensajería chinas *WeChat* y *Tencent QQ*, cuentan con su infraestructura de juegos para el desarrollo del metaverso, a partir de sus aplicaciones y su utilización en nuevos proyectos, apuntando a los juegos en el metaverso sustentado más en las soluciones de *software* que en *hardware* de realidad virtual (Binance Academy, 2021k).

Tecnologías que impulsan el metaverso

Toda la complejidad que involucra la construcción de la experiencia de la realidad virtual y el metaverso, implica la integración de diversos

ámbitos de los avances tecnológicos, entre los cuales se señalan algunos de los más importantes.

Realidad aumentada y Realidad virtual

Capaces de brindar una experiencia tridimensional, la realidad aumentada y la realidad virtual son puntos de entrada al mundo virtual. La realidad aumentada utiliza elementos visuales y personajes digitales para transformar el mundo real y puede utilizarse en casi cualquier teléfono inteligente o dispositivo digital con cámara.

Por intermedio de las aplicaciones de realidad aumentada, los usuarios pueden interactuar con imágenes digitales en su entorno real, similar a lo que se encuentra en un juego para celulares. En el caso de la realidad virtual se genera un entorno virtual totalmente por computadora, el cual los usuarios pueden explorar a través de la utilización de elementos de hardware como auriculares, guantes y sensores de realidad virtual (figura 21) (Binance Academy, 2021i).

Ambas representan modelos de metaverso que continuarán avanzando para expandir sus funcionalidades y alcance, fortaleciendo experiencia de los usuarios.

Inteligencia artificial

Los algoritmos de inteligencia artificial cuentan con la capacidad de procesar rápidamente gran cantidad de datos que, combinada con las técnicas de aprendizaje automático, pueden aprender de iteraciones anteriores a partir de datos históricos para generar resultados y conocimientos únicos.

En el ámbito del metaverso, se puede aplicar a los personajes no jugadores que existen en casi todos los videojuegos como parte del entorno, los cuales se diseñan para reaccionar y responder ante las actuaciones de los jugadores. Esto permitiría facilitar conversaciones realistas con

los usuarios y realizar otras tareas específicas, ejecutadas por sí solos (en distintos idiomas) y utilizadas por millones de jugadores de forma simultánea. Otra posible aplicación es la creación de avatares de metaverso, más realistas y precisos, con diferentes expresiones faciales, peinados, ropa y características que permitan mejorar los humanos digitales (Binance Academy, 2021i).

Figura 21
Aplicación de realidad virtual



Nota. Tomado de Huidobro (2021). Imagen de RODNAE Productions.

Reconstrucción 3D

Aunque esta tecnología no es nueva, su uso ha aumentado durante la pandemia, con particular énfasis en la industria de los bienes raíces, debido a las restricciones de las visitas presenciales de las personas interesadas en su adquisición, por lo que el uso de esta tecnología facilitó los recorridos virtuales en las propiedades. El reto en el ámbito del metaverso

es la creación de entornos virtuales con la mayor similitud posible al mundo real, con la representación de modelos fotorrealistas utilizando datos espaciales 3D y fotografía en alta definición que puedan ser procesadas para generar réplicas virtuales de objetos y lugares del mundo físico, con la finalidad de ofrecer a los usuarios (Binance Academy 2021g, 2021h).

Blockchain y criptomonedas

Como ya se ha mencionado, la tecnología *blockchain* tiene la capacidad de otorgar al metaverso una respuesta descentralizada y transparente a la protección de las características de propiedad digital, coleccionabilidad digital, transferencia de valor, gobernanza, accesibilidad e interoperatividad. De igual manera, las criptomonedas y NFT son elementos fundamentales que permiten a los usuarios las transacciones y la transferencia de valor, tanto en el mundo real como en el virtual. En el futuro, las criptomonedas pueden incentivar el trabajo en el metaverso, en la medida que se incorporen más empresas a poner sus oficinas en línea para el trabajo remoto (Binance Academy, 2021g, 2021h).

Internet de las cosas (IoT)

Consiste en un sistema a través del cual se toman los distintos elementos del mundo físico y se conectan a Internet mediante sensores y dispositivos, donde cada uno cuenta con un identificador único y la capacidad de enviar o recibir información de forma automática. Una de sus posibles aplicaciones en el metaverso es recopilar y proporcionar datos del mundo físico, aumentando la precisión de las representaciones digitales.

Su implementación permitiría la conexión del mundo 3D a una gran cantidad de dispositivos de la vida real, dando lugar a la creación de simulaciones en tiempo real en el metaverso. Si se conjuga con inteligencia artificial y aprendizaje automático para el procesamiento de tales datos, se lograría una mayor optimización del entorno en el metaverso (Binance Academy, 2021i).

Aplicaciones y usos del metaverso

Las circunstancias derivadas de la pandemia obligaron a la sociedad a avanzar en un proceso de adaptación a las nuevas circunstancias, en las cuales la búsqueda del equilibrio entre el resguardo de la vida y el desarrollo de la actividad económica potenció el uso de la tecnología y la superación de barreras que habían limitado su utilización en una gran cantidad de actividades, donde el papel de internet ha sido el elemento clave.

Aunque hoy en día ya no resulta extraño realizar entrevistas de trabajo, trabajar, comprar, aprender, jugar, asistir a conciertos, visitar museos y monumentos, y mucho más desde casa, solo se está ante una muestra de todo el potencial que metaverso puede ofrecer. De allí a continuación se presenta algunos de los usos y aplicaciones en los cuales se evidencian su influencia.

- Conciertos: ofrecería la posibilidad de ingresar y participar de manera virtual en un concierto en 3D. Por ejemplo, en 2019 el rapero Travis Scott protagonizó un concierto en *Fortnite* donde reunió alrededor de 100 000 usuarios en línea (Orellana, 2022).
- Trabajo: No solo se tratará de realizar entrevista o ejecutar tus tareas desde casa, se podría crear tu propio espacio u oficina (por ejemplo, a través de *Infinite Office* de Facebook), ingresar a una oficina en 3D, asistir a reuniones, interactuar con los avatares de tus colegas o trabajar directamente en el metaverso, recibiendo tu pago en utilizables en el mismo entorno o realizable a dinero fiduciario (figura 22). De hecho, en la actualidad existe este tipo de trabajo de una manera similar (Binance Academy, 2021g; Huidobro, 2021; Orellana, 2022).
- Videojuegos: en la actualidad existen juegos como *Axie Infinity*, *The Sandbox* y *Decentraland* cuentan con aspectos del metaverso e incorporan elementos de la vida real al virtual. Algunos incluso con modelos “juega para ganar” (*play-to-earn*) ofrecen la posibilidad de que el usuario genere NFT o monedas virtuales intercambiables y transables, susceptibles de ser convertidas en dinero fiduciario en

el mundo real, transformándose en un trabajo. También podría obtenerse una recompensa en un videojuego que luego pueda exhibirlo en otras instancias del mismo metaverso, para mostrárselo a amigos virtuales (Huidobro, 2021; Binance Academy, 2021g, 2021h).

- Educación: en este ámbito se presenta la oportunidad de aprovechar las potencialidades de abordar el aprendizaje desde aproximaciones más dinámicas y con posibilidad de adentrarse en los distintos fenómenos a analizar. A pesar de no ser los más publicitados, se han desarrollado diversas investigaciones en las cuales se involucran los avatares, realidad virtual y metaversos en los procesos de aprendizaje significativos en distintos niveles y áreas de conocimiento, como los realizados por Cárdenas Espinosa (2014), Anacona *et al.* (2019), Jaramillo-Mujica *et al.* (2017), Fernández-Blanco Martín, (2016), entre otros.

Figura 22
Oficina en realidad virtual



Nota: Tomado de Huidobro (2021). Imagen de *ThisIsEngineering.*

Las aplicaciones y usos anteriores son solo algunos de los existentes, sin hablar del obvio empleo en simuladores cada vez más reales, en el campo de la salud física y mental, así como en las diferentes posibilidades en los ámbitos civil y militar.

Ejemplos de metaverso

Decentraland

En 2016, la plataforma de código abierto se inició con un experimento en 2D básico que se ha venido desarrollando hasta el gran mundo virtual en 3D de la actualidad. Sus desarrolladores Esteban Ordano y Ari Meilich han creado un espacio online que combina la realidad virtual con la tecnología de *blockchain*. *Decentraland* contiene parcelas de bienes raíces digitales, artículos y otros activos personalizables, los cuales se pueden comprar con *MANA* (figura 23), el *token* ERC-20 (NFT) de la plataforma, que además representan objetos coleccionables del juego como ropa, artículos y espacio virtual del juego *LAND* (terreno). Puede comprarse en diversos *exchanges*, tanto con criptomonedas como con moneda *fiat* (Binance Academy, 2021i, 2021g).

Figura 23
Moneda de Decentraland MANA



Nota. Tomado de Binance Academy (2021j).

Los *tokens* además de ser el dinero del juego que los usuarios almacenan en sus billeteras virtuales, pueden comercializarlas y venderlas incluso por altas cifras de dinero, por lo que también es posible ganar dinero. Además, los jugadores que tienen *tokens* participan en la definición de las reglas que rigen este mundo virtual, a través de votación directa acerca de las políticas organizativas y del juego en sí, mecanismo que afecta desde los tipos de elementos permitidos hasta las inversiones para la tesorería.

El juego cuenta con cinco usos principales basados en *blockchain* incluidos en el proyecto por sus desarrolladores (Binance Academy, 2021j), a saber:

- Aplicaciones: los usuarios pueden crear aplicaciones y escenas en 3D con el lenguaje de secuencias de comandos de *Decentraland*, proporcionando mejores interacciones.
- Curación de contenido: en *Decentraland* se han desarrollado vecindarios, atrayendo a fanáticos de ideas afines y comunidades orgánicas en crecimiento.
- Publicidad: el tráfico de jugadores en los vecindarios ha atraído a las marcas a comprar espacios publicitarios y coloquen vallas publicitarias (figura 24).

Figura 24
Imagen de Decentraland



Nota: Tomado de Binance Academy (2021j).

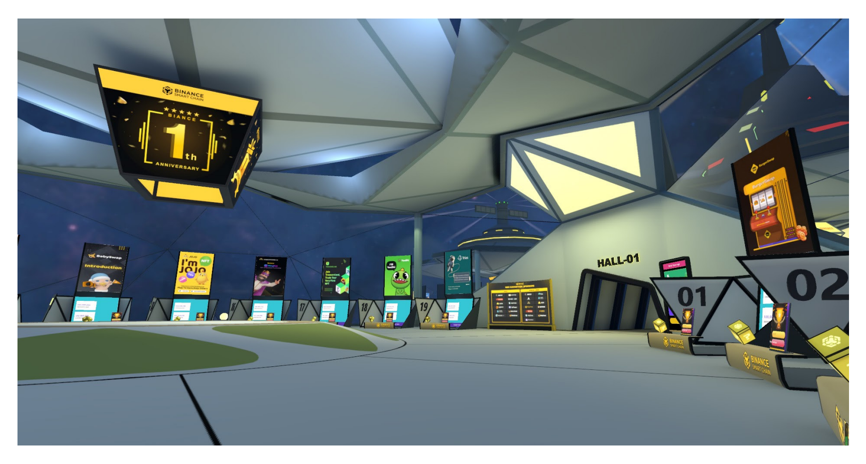
- Coleccionables digitales: los artículos NFT se recopilan, crean y comercializan en *Decentraland Marketplace*, proporcionando derechos de propiedad a los usuarios.
- Social: las comunidades en plataformas de redes sociales o incluso grupos *offline* (sin conexión) pueden contar con una manera más interactiva de socializar con sus amigos.

Second Live

Consiste un entorno virtual 3D, en el cual los usuarios pueden vivir una vida paralela a través de avatares que les permite socializar, aprender y hacer negocios en la plataforma. Cuenta con un mercado NFT para el intercambio de objetos coleccionables (figura 25 y figura 26). También han incursionado en la organización de exposiciones y eventos virtuales como el *Harvest Festival* en 2020 (Binance Academy, 2021h).

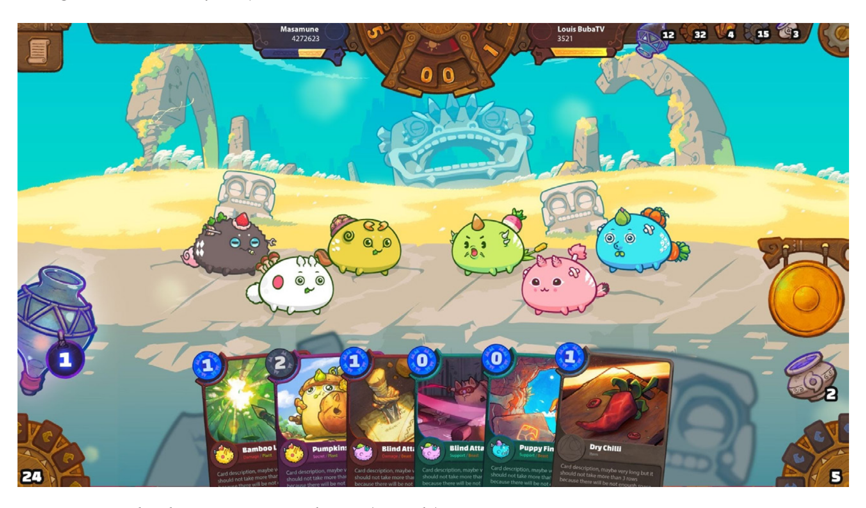
Figura 25

Imagen de Second Live



Nota. Tomado de Binance Academy (2021h).

Figura 26
Imagen de Axie Infinity



Nota. Tomado de Binance Academy (2021h).

Axie Infinity

Se trata de un juego coleccionable creado en 2018. *Axie Infinity Shard* (AXS) es el *token* del ecosistema, el cual fue lanzado en 2020. Los *tokens* AXS se pueden comprar, intercambiar o ganar durante el juego como recompensa a los principales jugadores. También cuenta con otros activos del juego (*Axies*) en forma de NFT que puedes guardar en tu billetera, así como *Smooth Love Potion* (SLP), un *token* que se han popularizado porque permite generar ingresos constantes a los jugadores solo por jugar *Axie Infinity*. Al venderse en el mercado abierto, se podría ganar aproximadamente entre $200 y $1000, dependiendo de cuánto juegues y de su precio en el mercado. Si bien en *Axie Infinity* no proporciona un personaje o avatar singular en 3D, brinda a los usuarios la oportunidad de un trabajo similar al metaverso (Binance Academy, 2021g, 2021k).

Retos y riesgos asociados a la tecnología del metaverso

Todo avance tecnológico trae consigo retos y riesgos relacionados con comportamientos oportunistas que surgen en la medida que se divulga en la sociedad, más aún si se trata de cambios que están en pleno desarrollo. Es así que se han identificado algunos aspectos, a saber:

- Autenticación de identidad y control de la privacidad: a medida que las personas incursionan en el mundo digital con avatares, es difícil saber o demostrar la identidad de la otra persona, trayendo consigo riesgos de que personas actúen indebidamente o incluso *bots* podrían ingresar al metaverso asumiendo la identidad de otra persona con la finalidad de ocasionar daño a su reputación de esa persona o estafar a otros usuarios.
- En este mismo orden de ideas, el acceso de los dispositivos de realidad aumentada y realidad virtual a cámaras e identificaciones únicos, pueden ser objeto de accesos no autorizados y filtraciones no deseadas de información personal de los usuarios, como en efecto ha ocurrido (Binance Academy, 2021i).
- Desembolso económico: se requiere realizar una inversión en los software y hardware para poder acceder al metaverso, montos que resultan altos para la mayoría de las personas, lo cual trae como consecuencia un aumento de la brecha digital (Huidobro, 2021).
- Repercusiones emocionales o psicológicas: aspectos relacionados con el sedentarismo y pérdidas de las relaciones sociales presenciales pueden verse seriamente afectados por los usos del metaverso, aun cuando estos incluyan cierto tipo de actividad física. Además, la mayor vulnerabilidad de algunos sectores de la población ante las interacciones en el mundo virtual, tales como personas que han sufrido brotes psicóticos o epilépticos, nativos digitales y personas que no perciben peligro en las redes sociales; siendo de especial atención los niños y adolescentes que pueden desarrollar adicciones a las compras, redes sociales o juegos, que en algunos casos ya han ocasionado hasta la muerte (Huidobro, 2021; Organización Mundial de la Salud, 2022).

- Adaptación de las leyes: aspecto que se ha planteado en temas como privacidad y protección de datos, propiedad intelectual, derechos de usuarios electrónicos, entre otros. Sin embargo, también se exponen opiniones que se pronuncian a la adaptación de la normativa existente a las nuevas realidades derivadas de la naturaleza de las interacciones en el metaverso.
- Monopolización del metaverso: la posibilidad de que una o pocas empresas tomen el control del metaverso como coincidencia del mundo virtual y el mundo real, representa una herramienta muy poderosa en manos de intereses particulares, con el potencial de generar matrices de opinión, cambiar la mentalidad de las personas e influir significativamente en los distintos ámbitos de la vida, especialmente los más susceptibles como adolescentes (Huidobro, 2021).

Conclusiones

Al hablar de tecnología, efectivamente se piensa en avances. No cabe duda de que la aparición del *bitcoin* basada en la aplicación de la tecnología de la cadena de bloques (*blockchain*) como medio para otorgarle sus características de base de datos distribuida, transmisión entre iguales, transparencia con seudonimato, irreversibilidad de los registros y lógica computacional, ha transformado la dinámica económica mundial, abriendo un potencial de posibles aplicaciones tanto en los sectores público y privad, así como en las organizaciones no gubernamentales.

La tecnología del *blockchain*, las criptomonedas y el metaverso se encuentran en pleno desarrollo y pueden realizar aportes importantes en una variedad de actividades, sectores, e industrias. La cadena de bloques puede aportar transparencia y seguridad, especialmente en el manejo de recursos en el sector público y las organizaciones no gubernamentales.

A pesar de los progresos en la aceptación de las criptomonedas como forma de pago y reserva de valor, existen múltiples temas pendientes cuya tendencia pudiera afectar a los propios principios en los que se sustentan. Su funcionamiento en la forma de una red distribuida y el seudonimato puede verse debilitado. En la medida que se requieren mayores inversiones en equipos costosos con la suficiente potencia computacional para almacenar las bases de datos y procesar rápidamente las transacciones que le permitan a los nodos lograr rendimientos suficientes para recuperar lo invertido, también merma el número de usuarios en función de su capacidad financiera. Esto sugiere la concentración de los nodos en menos manos, lo que aumenta la posibilidad de ataques al 51 %.

La extrema volatilidad de sus precios, susceptible de situaciones como la opinión de algunas personalidades, instituciones o gobiernos acerca de ellas y su uso, es un tema sobre el cual no se han hecho esfuerzos suficientes. La ausencia de terceros para la ejecución de las transacciones es otro tema que está entrando en contradicción. Las billeteras digitales están asumiendo un rol similar a los bancos tradicionales, de custodia e intermediación financiera, que son parte de las razones principales que dieron origen a las criptomonedas.

Dado que aún queda mucho por desarrollarse en cuanto a las criptomonedas, existen otros temas importantes sobre los que hay que alertar: la ineficiencia en la utilización de los recursos particularmente los energéticos, la inversión en adquisición en infraestructura tecnológica y la accesibilidad real de personas e instituciones para incorporarse a esta nueva dinámica, el fraude, el lavado de dinero, el financiamiento de actividades ilícitas, por nombrar solo algunos.

En cuanto a los *tokens* no fungibles (NFT), han ganado popularidad por su relación con los juegos que le dieron origen, debido a sus funcionalidades dentro los propios juegos. Además, el atractivo de coleccionarlos e intercambiarlos están conformando un mercado cada vez más valioso, permitiendo generar ingresos, en ocasiones, muy importantes. Sus aplicaciones como elemento de certificación de autenticidad y propiedad están tomando relevancia en la construcción del metaverso, aunque aún se encuentran por desarrollarse y aceptarse en el mundo real.

La introducción de la tecnología del *blockchain* y sus aplicaciones ha dado origen a la creación de criptomonedas, contratos inteligentes (*smart contracts*) y *tokens* no fungibles (NFT), transformándose en un factor clave en el desarrollo del metaverso.

Se trata de avances tecnológicos que están revolucionando la forma de hacer negocios, la dinámica social y económica de las personas, las organizaciones y los países, representando grandes retos en virtud de sus implicaciones en cuanto a sus potenciales aplicaciones en favor de la

población y la forma cómo se establecen las relaciones en los distintos ámbitos, así como los riesgos en materia económica, social, legal, psicológica, utilización de los recursos, lavado de dinero, financiamiento al terrorismo, entre otros.

Referencias bibliográficas

Allende, M. y Colina, V. (2018). *Blockchain cómo desarrollar confianza en entornos complejos para generar valor de impacto social.* Banco Interamericano de Desarrollo, ITE/IPS Techlab. https://bit.ly/3mjy7qy

Almonacid Sierra, J. y Coronel, Y. (2020). Aplicabilidad de la inteligencia artificial y la tecnología blockchain en el derecho contractual privado. *Revista de Derecho Privado,* (38), 119-142. https://bit.ly/3ZlOp0S

Anacona, J. D., Millán, E. E. y Gómez, C. A. (2019). Aplicación de los metaversos y la realidad virtual en la enseñanza. *Entre Ciencia e Ingeniería, 13*(25), 59-67. doi:https://doi.org/10.31908/19098367.4015

Arango, C. A., Bernal, J. F., Boada, A. y Barrera, M. M. (2018). *Criptoactivos.* Bogotá.

Armstrong, B. (25 de julio de 2018). Is coinbase creating a centralized or decentralized financial system? *Traders Magazine.* http://bit.ly/3YklA3g

Arrasco Arteaga, H. (2021). *Tecnologías Blockchain. Innovación Empresarial y Aplicación.* Trabajo de Grado, Universidad Politécnica de Cataluña. https://bit.ly/3Zy8NMp

Bech, M. y Garratt, R. (2017). Criptomonedas de bancos centrales. *Boletín CEMLA.* https://bit.ly/3kH0mPB

Berryhill, J., Bourgery, T. y Hanson, A. (s.f.). Blockchains unchained: Blockchain tecnology and its use in the public sector. *OECD Working Papers on Public Governance* (28). https://bit.ly/3FgIJNJ

Binance Academy. (2018a). *La historia de Blockchain.* https://academy.binance.com/es/articles/history-of-blockchain

Binance Academy. (13 de diciembre de 2018b). *¿Qué es un algoritmo de consenso?* https://academy.binance.com/es/articles/what-is-a-blockchain-consensus-algorithm#proof-of-work-pow

Binance Academy. (4 de diciembre de 2018c). *¿Qué son las criptomonedas?* https://academy.binance.com/es/articles/what-is-cryptocurrency

Binance Academy. (4 de diciembre de 2018d). *Ventajas y desventajas del blockchain.* https://academy.binance.com/es/articles/positives-and-negatives-of-blockchain

Binance Academy. (7 de diciembre de 2018e). *¿Qué es Trust Wallet?* https://academy.binance.com/es/articles/what-is-trust-wallet

Binance Academy. (15 de septiembre de 2019a). *¿Qué son los smarts contracts?* https://academy.binance.com/es/articles/what-are-smart-contracts

Binance Academy. (17 de junio de 2019b). *¿Qué es una billetera de criptomonedas?* https://academy.binance.com/es/articles/crypto-wallet-types-explained

Binance Academy. (23 de febrero de 2020a). *¿Qué es Bitcoin?* https://academy.binance.com/es/articles/what-is-bitcoin

Binance Academy. (25 de febrero de 2020b). *Una guía sobre cripto-coleccionables y tokens no fungibles (NFT).* https://academy.binance.com/es/articles/a-guide-to-crypto-collectibles-and-non-fungible-tokens-nfts

Binance Academy. (30 de agosto de 2021a). *9 Altcoins para diversificar tu portafolio.* https://academy.binance.com/es/articles/altcoins-to-diversify-your-portfolio

Binance Academy. (2021b). *Guía sobre monedas digitales de bancos centrales (CBDC).* https://academy.binance.com/es/articles/central-bank-digital-currencies-cbdc-explained

Binance Academy. (15 de noviembre de 2021c). *¿Qué son monedas meme?* https://academy.binance.com/es/articles/what-are-meme-coins

Binance Academy. (22 de junio de 2021d). *¿Por qué Bitcoin tiene valor?* https://academy.binance.com/es/articles/why-does-bitcoin-have-value

Binance Academy. (27 de abril de 2021e). *Cómo crear tus propios NFTs.* https://academy.binance.com/es/articles/how-to-make-your-own-nfts

Binance Academy. (30 de julio de 2021f). *Las mejores billeteras de criptomonedas para Binance Smart Chain (BSC).* https://academy.binance.com/es/articles/the-best-crypto-wallets-for-binance-smart-chain-bsc

Binance Academy. (28 de mayo de 2021g). *Los 7 casos de uso principales de NFT.* https://academy.binance.com/es/articles/top-7-nft-use-cases

Binance Academy. (21 de septiembre de 2021h). *¿Qué es el metaverso?* https://academy.binance.com/es/articles/what-is-the-metaverse

Binance Academy. (22 de diciembre de 2021i). *Las 7 principales tecnologías que impulsan el metaverso.* https://academy.binance.com/es/articles/top-7-technologies-that-power-the-metaverse

Binance Academy. (5 de mayo de 2021j). *¿Qué es Decentraland (MANA)?* https://academy.binance.com/es/articles/what-is-decentraland

Binance Academy. (8 de diciembre de 2021k). Seis empresas globales que construyen el metaverso. https://academy.binance.com/es/articles/global-companies-building-up-the-metaverse

Binance Academy. (3 de febrero de 2021l). *¿Qué es Axie Infinity (AXS)?* https://academy.binance.com/es/articles/what-is-axie-infinity-axs

Bit2me Academy. (s.f.). *¿Qué son las DAPPs?* https://academy.bit2me.com/que-son-las-dapps/

Bogart, S. y Rice, K. (2015). *The blockchain report: welcome to the internet of value.* Needham Insights.

Böhme, R., Christin, N., Edelman, B. y Moore, T. (2015). Bitcoin: Economics, Technology and Governance. *Journal of Economic Perspectives, 29*(2), 213-238. http://bit.ly/3IMmcsW

Bolaños, J., Luetticke, F. y Galarza, J. (2019). *Criptoeconomía: Cómo el bitcoin y blockchain están cambiando al mundo y tus finanzas* (1 ed.). https://bit.ly/3KTpkWH

Bullón Pérez, J. J., Queiruga-Dios, A., Gayoso Martínez, V. y Martín del Rey, Á. (2020). Traceability of ready-to-wear clothing through blockchain technology. *Sustainability, 12*(18), 74-91. http://bit.ly/3EVBYAx

Cabrera Valencia, F. (2018). *Tecnología Blockchain: elementos básicos, aplicaciones y marcos regulatorios.* Biblioteca del Congreso Nacional de Chile. https://bit.ly/3y9LcWg

Carbonero del Val, M. (2021). *El blockchain, un impulso de desarrollo para el sector retail.* (Trabajo de Grado). Comillas Universidad Pontificia. https://bit.ly/3ZFaIOu

Cárdenas Espinosa, R. D. (2014). Metaversos y su relación en el aprendizaje significativo a través de los avatares. *I Bienal Latinoamericana de Infancias y Juventudes. Democracias, Derechos Humanos y Ciudadanías.* Universidad de Manizales-CLACSO. http://bit.ly/3kJRRTL

Carlozo, L. (13 de junio de 2017). Why CPAs need to get a grip on blockchain. *Journal of Accountancy*. http://bit.ly/3ETcMe7

Catalini, C. (2017). How Blockchain applications will move beyond finance. *Harvard Business Review.* http://bit.ly/3YnVXi1

CEDICE Libertad. (2021). *Manual de Blockchain. Cadena de bloques y tecnología. Herramienta para la transparencia y el fortalecimiento institucional para sector público, privado y sociedad civil.* Caracas. https://bit.ly/3Zxts2o

Ciaian, P., Rajcaniova, M. y Kancs, d'A. (2016). The economics of BitCoin price formation. *Applied Economics, 48*(19), 1799-1815. http://doi.org/10.1080/00036846.2015.1109038

Ciaian, P., Rajcaniova, M. y Kancs, d'A. (2018). Virtual relationships: Short- and long-run evidence from BitCoin and altcoin markets. *Journal of*

International Financial Markets, Institutions and Money, 52, 173-197. http://doi.org/10.1016/J.INTFIN.2017.11.001

Domínguez, J. y García R. (2018). Blockchain y las criptomonedas: el caso bitcoin. *Revista de los estudios de economía y empresa, 10*, 58-73. https://n9.cl/nvnyy

El Economista. (26 de enero de 2022). El FMI alerta de los "grandes riesgos" de adoptar bitcoin como moneda y El Salvador responde subiendo la apuesta. *El Economista*. http://bit.ly/3kDfi1b

Ethereum. (2022). http://bit.ly/3ETf4Kf

European Central Bank. (2015). *Virtual currency schemes: a further analysis*. https://bit.ly/3J7LUJN

Fernández Hurtado, S. R., Vila Pacheco, A., Arboleda, K. L., Garcés, J. C. y Martínez Martínez, L. Á. (2021). Relación entre la alcoint y el bitcoin: Análisis de mayor liquidez. En S. R. Fernández Hurtado y J. Portocarrero Cuero, *Monedas disruptivas: Atractivo financiero y tecnológico* (pp. 13-45). Universidad Santiago de Cali. https://doi.org/10.35985/9789585147799

Fernández-Blanco Martín, G. (2016). *Procesos creativos en entornos musicales inmersivos: un estudio de caso a través del análisis de metaversos. La Avatar Orchestra Metaverse en Second Life*. Universidad Complutense de Madrid. http://bit.ly/3ZuXzYE

Financial Action Task Force. (2014). *Monedas virtuales. Definiciones Claves y riesgos potenciales de LA/FT*.

Floyd, D. (3 de septiembre de 2018). 10 years after Lehman: Bitcoin and Wall Street Are Closer than Ever. *Coindesk*.

Grupo Garatu It Solutions. (8 de noviembre de 2018). *¿Qué tipos de Blockchain o cadenas de bloques existen?* https://bit.ly/3y9PGw4

Gutiérrez, F. (2019). *Qué es blockchain: cómo funciona la tecnología detrás de Bitcoin*. http://bit.ly/3KUJzDo

Haber, S. y Stornetta, S. W. (1991). How to time-stampl a digital document. En A. J. Menezes, y S. A. V, *Advances in Cryptology-CRYTO'90. CRYPTO 1990* (Vol. 537). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-38424-3_32

Halaburda, H. y Sarvary, M. (2016). *Beyond bitcoin: The economics of digital currencies*. MacMillan.

Huidobro, M. (2 de diciembre de 2021). Metaverso: qué es, qué ofrece y qué retos plantea. http://bit.ly/3IQ3cdb

Huillet, M. (31 de octubre de 2019). Hoy se cumplen 11 años del día en que Satoshi Nakamoto publicó el White paper del Bitcoin. *CoinTelegraph*. https://bit.ly/3midkUh

Jaramillo-Mujica, J. A., Morales-Avella, L. F. y Coy-Mondragón, D. M. (2017). Una experiencia en el uso de metaversos para la enseñanza de la física mecánica en estudiantes de ingeniería. *Revista Educación en Ingeniería, 12*(24), 20-30. https://doi.org/10.26507/rei.v12n24.778

Kolvart, M., Poola, M. y Rull, A. (2016). Smart contracts. En *The future of law and etechnologies* (pp. 133-147). Springer, Cham.

Lamothe Fernández, P. y Lamothe López, P. (2020). ¿Cómo valorar los denominados criptoactivos? *Cuadernos de Información Económica, 277,* 71-80, julio/agosto. https://bit.ly/3ZEkLU2

Leal, A. (17 de febrero de 2022). ¿Qué es una wallet de bitcoin y criptomonedas?. https://www.criptonoticias.com/criptopedia/que-es-wallet-bitcoin-criptomonedas/

Linares-Barbero, M. (2019). Trazabilidad con Blockchain. En Hacia la transformación digital. Universidad de Lima (ed.), *Actas del I Congreso Internacional de Ingeniería de Sistemas* (pp. 99-106), Lima, 13 y 14 de septiembre del 2018. Universidad de Lima, Fondo Editorial.

Lindman, J., Berryhill, J., Welby, B. y Marbieri, M. P. (2020). The uncertain promise of blockchain for government on Public Governance. *OECD Working Papers, 43*(Nov). https://bit.ly/3EVJ08i

López Gómez-Cadiñanos, T. (2021). *Criptomonedas y Blockchain.* (Trabajo Fin de Grado). Universidad de Oviedo. https://bit.ly/3EVJs6u

Maceo Herrera, R. (2021). Blockchain, una tecnología disruptiva hacia el Internet de generación de valor. *Revista Tono, 17*(1), 30-41. https://bit.ly/3Yj9Iyw

Maldonado, J. (16 de julio de 2020). DLT vs Blockchain. *CoinTelegraph.* https://bit.ly/3J7SxMa

McCoy, S. (23 de octubre de 2019). Un nuevo Haskell reescrito para Cardano. https://n9.cl/wzhig

Moore, T. y Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. En A.-R. Sadeghi, *Lecture Notes in Computer Science* (pp. 25-33). Springer-Verlag.

Morales, J. (8 de noviembre de 2021). Sobre Cardano, EMURGO y IOHK. https://cryptoticker.io/es/sobre-cardano-emurgo-y-iohk/

Muñoz Moreno, P. (2020). *La irrupción de blockchain en la propiedad industrial e intelectual.* http://bit.ly/3SL2TEQ

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* https://bitcoin.org/bitcoin.pdf NO FUNCIONA LINK

OECD. (2018). OECD Blockchain Premier. *OECD.* https://bit.ly/3ZxdWng

Orellana, R. (11 de febrero de 2022). Qué es el metaverso y quiénes lo impulsan. http://bit.ly/3Zo6H1l

Organización Mundial de la Salud. (2022). *CIE-11 para las estadísticas de mortalidad y morbilidad (CIE-11 EMM).* http://bit.ly/3YgNxJy

Otero, M. (24 de noviembre de 2022). Criptomoneda ADA: Opinión y Características de Cardano. https://sincomisiones.org/trading/ada-cardano

Parra, J. A., Arango, C., Bernal, J., Gómez, J. E., Gómez, J., León, C., Machado, C., Osorio, D., Rojas, D., Suárez, N. y Yanquen, E. (2019). *Criptoactivos: análisis y revisión de literatura.* Banco República. https://bit.ly/3ZEOU5Y

Pieters, G. y Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets. *Information Economics and Policy, 39*, 1-14. http://doi.org/10.1016/J.INFOECOPOL.2017.02.002

Pontificia Universidad Javeriana. (s/f). Fundamentos de la tecnología blochain. https://bit.ly/3ZeyDoi

Presidencia de la República. (6 de agosto de 2021). Decreto Nº 4.553, mediante el cual se decreta la nueva expresión monetaria. *Gaceta Oficial de la República Bolivariana de* Venezuela (42.185). http://bit.ly/3mpEJnq

Preukschat, A. (2017). Ethereum es Turing completo ¿y eso qué es?. https://n9.cl/defct

Preukschat, A., Kuchkovsky, C., Gómez, G. y Díez, D. (2017). *Blockchain. La revolución industrial de internet.* Grupo Planeta.

Puig, A. (2018). Tipos de Blockchain y casos de uso. *Foro Innovación en Tecnologías Disruptivas.* España.

Real Academia de la Lengua Española. (2022). *Diccionario de la Real Lengua Española.* https://bit.ly/3INX4lv

Rodríguez Quejido, V. (2019). *Criptoactivos: naturaleza, regulación y perspectativas.* Documento de trabajo Nº 29, Instituto de Estudios Financieros, Observatorio de Divulgación Financiera, Barcelona. España. https://bit.ly/3ETmDR9

Rodríguez, N. (2019). *Blockchain Como Servicio - BAAS: Soluciones de Nivel Empresarial.* https://bit.ly/3EPUIRW

Romo Conde, L. (2021). *Análisis económico de criptoactivos y tecnología blockchain.* (Trabajo Fin de Grado). http://bit.ly/3Yo46mB

Rus, E. (1 de noviembre 2021). Litecoin (LTC). https://economipedia.com/definiciones/litecoin-ltc.html

Sáez, J. (1 de julio de 2021). ¿Qué son las DLT y en qué se diferencian de Blockchain? *IEBS.* https://bit.ly/3mrwGqg

Schwartz, D., Youngs, N. y Britto, A. (2014). *The Ripple Protocols Consensus Algorithm.* https://arxiv.org/abs/1802.07242

Tecno Global Solution. (6 de julio de 2020). ¿Qué es el Bitcoin? https://tglsolution.com/2020/07/06/que-es-el-bitcoin/

Vázquez, C. (14 de junio de 2019). Los cinco mejores Pools para minar Litecoin ahora mismo. https://n9.cl/w826e

Vigna, P. y Casey, M. (2016). *The Age of Cryptocurrency.* St. Martin Press.

Sobre autores



Narcisa Jessenia Medranda Morales es Doctora (Ph.D.) en Comunicación y Periodismo por la Universidad Autónoma de Barcelona, es Magíster en Periodismo Investigativo, Datos y Visualización por la Universidad Internacional de la Rioja, tiene una Maestría en Educación de la Universidad de León. Es Licenciada en Comunicación Social por la Universidad Politécnica Salesiana.

Durante su trayectoria académica, se destacó por investigar el tema de la calidad y transparencia en la información y comunicación emitida en las páginas web de los municipios, comparando casos de Ecuador y España. Actualmente, es Directora y docente de las carreras de Comunicación y Diseño Multimedia, así como docente de la Maestría en Comunicación Estratégica Digital en la sede Quito, Cuenca y Guayaquil de la Universidad Politécnica Salesiana. Además, forma parte del grupo de investigación CODEPO de la misma institución.

Narcisa Medranda Morales es autora de varios artículos publicados en JCR, Scopus y Latindex, así como más de 30 capítulos de libro en diferentes editoriales. Además, es autora del libro "El poder en las manos de la ciudadanía", coordinadora de los libros Comunicación y ciudad, "Ecología de la información I y II" y Comunicación, política y desarrollo". Su destacada trayectoria académica la convierte en una experta en su campo y una figura importante en la comunidad académica de la comunicación.



Miguel Arcos Argudo es Doctor en Ciencias de la Computación para Smart Cities, Máster en Seguridad de las Tecnologías de la Información de las Comunicaciones, Máster en Ciencias de la Computación, es Ingeniero de Sistemas. Es Director de la Maestría en Seguridad de la Información de la UPS. Docente Investigador de la UPS, tiene a sus haberes varias investigaciones de alto impacto

Carrera de Comunicación

¿Qué son el blockchain, los criptoactivos y el metaverso? ¿Cómo funcionan y cómo impactan en nuestra sociedad? Este libro explora estos temas y ofrece una aproximación teórica a estos fenómenos tecnológicos y culturales de la actualidad.

A través de un análisis riguroso y accesible, Narcisa Medranda y Miguel Arcos nos introducen en el mundo del blockchain, la tecnología que está detrás de los criptoactivos como Bitcoin, Ethereum y otras criptomonedas. Profundizan en el concepto del metaverso, un espacio virtual que se está convirtiendo en una nueva dimensión de la experiencia humana; nos hacen descubrir cómo el blockchain está cambiando la forma de gestionar las transacciones convirtiéndose en una herramienta para la seguridad de la información en muchos sectores. Por último, exploran cómo los criptoactivos generan nuevas formas de inversión y de transacciones financieras.

Por otro lado, el libro analiza el impacto del metaverso en nuestra sociedad, desde su relación con la cultura digital y el ocio hasta su influencia en la economía global. ¿Cómo están cambiando estos fenómenos nuestra forma de entender el mundo y nuestra relación con la tecnología?





